Till Morfar

I dedicate this work to my grandfather, Bertil Fagerlund; your continued engagement in and care for the future, as an engineer and human being, are an inspiration.

Disassembling the Trust Machine

Three cuts on the political matter of blockchain

Jaya Klara Brekke

Abstract:

Blockchain technology is, in part, a proposal to resolve 'the political' through technical means: decentralised networks to solve the problem of authority; cryptography to coordinate and secure the network; and game theory and incentive design to solve network behaviour. This PhD thesis draws on theoretical work by Karen Barad (2007) and Jacques Rancière (Rancière, 2010) to ask the question of *what matters politically in blockchain technology* – both in the sense of matter as becoming material of a new mediation of the political, but also mattering in the sense of being of political importance to engineers, developers and communities forming around blockchain as a potential. Rather than treating blockchain as coherent thing to be either celebrated or criticised, this thesis proposes and attempts to draw out the ways in which the potentials of blockchain are negotiated as part of its political effects, looking towards these negotiations to understand how political differences are made and sought materialised. Three approaches to the political are articulated to analyse Bitcoin and Ethereum as case studies and shift their terms of debate. Firstly, addressing the question of algorithmic determinacy, an approach is proposed for critically understanding a blockchain proposition that does not immediately revert to a competition of control between 'human' and 'machine' through the notion of the *insensible,* drawing on work by geographer of the inhuman Yusoff (2013a). Secondly, drawing on political theorist Rancière (2010) a particular blockchain *sensibility* is articulated, addressing the question of the particular kind of 'disruption' that blockchain presents. Its specific provenance in political histories of decentralised network computation opens up political significance beyond its intersections with financial capitalism. Finally, addressing the question of blockchain as a resolution to the political, the thesis introduces the concept of *dissensible* as an ongoing potential for incompatible sensibilities and their negotiation.

Acknowledgements

The people who have taken an interest in my work throughout this PhD have been invaluable with regards to its shaping and completion. Making me write more and putting me on stage over and over again forced me to be technically and theoretically rigorous and gave me motivation and helped me find meaning in what I was looking to achieve. Thank you in particular to Elias Haase from *B9Lab*, Ruth Catlow from *Furtherfield and DECAL*, Ben Vickers of *Serpentine Gallery* and *Ignota Books*, Matthias Tarasiewicz, Andrew Newman, Markus Zimmerman and everyone at *RIAT, Institute for Future Cryptoeconomics*. I also want to acknowledge in particular Brett Scott, Kei Kreutler, Dan Hassan, Rachel Rose O'Leary and Adam Greenfield – for drawing me into your networks, seeing value in my work and being important allies. I would like to give a huge thanks to George Danezis and the *InfoSec* research group of UCL Computer Sciences department, for all the conversations and adopting me at a critical moment. Furthermore, many thanks to Harry Halpin and everyone involved with *NEXTLEAP* for involving me in the project that supported me in the final crucial months of writing. I want to acknowledge the important work and friendship of Francesca Bria, thank you for all the conversations and insights, inviting my involvement in *D-CENT*, my initial introduction to blockchain and *DECODE*, as blockchain advisor. I also want to acknowledge the insights and efforts of Denis 'Jaromil' Roio and Marco Sachy from the always on-point Think-And-Do-Tank, *Dyne*, and thank you Tomer Kantor of Proof-of-Work, for sharing your insights and recordings. Sincere thanks also to Mohammad Salemi, Patrick Schabus and everyone else at *The New Centre for Research and Practice,* Sonja Grdina, Janez Janša and Marcela Okretič and everyone at *Aksioma*. I have much appreciation for the unknown inventors of the *Pomodoro Technique* and to Pooya Ghoddousi for Pomodoros and planks at the British Library; these got me through the writing marathon, and Matthew Benson for those final months. Thank you Heather Parry for making sure my words and sentences make sense! I want to acknowledge the tireless work of Enric Duran, for the interest and openness; Anna Giralt Gris for hosting me and for the constant stream of energy and enthusiasm; and Sib and Monica for conversations that kept me real. Antonis Vradis, who I need to thank, (or blame); I would not have pursued an academic career if it hadn't been for your stubborn encouragement. To my London crew, especially Anya Eckbo, the most supportive and inquisitive friend one can hope for; thank you Will Kangpe, for the patient reading, the music and lifesaving juju; and Ross Domoney, for the writing retreats, annoying face-tapping and reminders of all colours, images, ocean and teargas beyond my computer screen. To Maria Fagerlund and Ole Brekke, to whom I owe it all; Karl Fagerlund Brekke, you keep me sane; Kathrine Fagerlund Brekke and Joel Brekke for your never-failing encouragement. Finally, I want to acknowledge the exceptional research environment, colleagues and fellow PhD candidates at the Geography Department of Durham University. Last but not least, to Joe Painter and Harriet Bulkeley, my PhD supervisors – thank you for your patience with my pile

of ‘slugs’, generosity of time and feedback, crucial encouragement and enough *trust* to let me meander through debates, places and literature that at times were rather far from the department in Durham. Responsibility for the content of this thesis rests solely with myself.

Music acknowledgements: Alva Noto, Ryuichi Sakamoto, Jasss, Djrum, Laurel Halo, Mica Levi, MF DOOM, Agnes Obel, Ta-ku, Arca, Jean Grae (Kill Screen!), Biig Piig, Blood Orange, Coucou Chloe, Emmanuelle Parrenin, Homeshake, Moses Sumney, Christine and the Queens, Ivo Dimchev, James Blake, Tirzah, Michelle Gurevich, SBTRKT, Sonic Youth, serpentwithfeet, DJ Cam, The Blaze, Melanie de Biasio, Micachu & The Shapes, Wayne Snow (to acknowledge some of the most repeated soundtracks that undoubtedly have shaped some of my neural pathways).

Abbreviations

DAO	Decentralised Autonomous Organisation
dApps	Decentralised Applications
STS	Science and Technology Studies
IoT	Internet of Things
US	United States of America
CIC	Cooperativa Integral Catalana
ATM	Automated Teller Machine
UCL	University College London
DDoS	Distributed Denial of Service
DHT	Distributed Hash Table
CPU	Central Processing Unit
ASIC	Application-Specific Integrated Circuit
EVM	Ethereum Virtual Machine
BBC	British Broadcasting Corporation
FBI	Federal Bureau of Investigation
ISP	Internet Service Provider
DLT	Distributed Ledger Technology
CIA	Central Intelligence Agency
TCP/IP	Transmission Control Protocol/Internet Protocol
DIY	Do It Yourself
ICO	Initial Coin Offering
KYC	Know Your Customer
AML	Anti Money Laundering
UK	United Kingdom
BIP	Bitcoin Improvement Proposal
EIP	Ethereum Improvement Proposal

Disassembling the Trust Machine

Three cuts on the political matter of blockchain

Jaya Klara Brekke

PhD Thesis

Geography Department

Durham University

2019

Table of Contents

1 Introduction

This thesis addresses the question of *the political* in and through a technology that claims to solve it. The fascinating proposition of blockchain technology lies in the ability of an algorithm to determine consensus across a decentralised network without resorting to an external authority for decision and enforcement. As such, blockchain technology has been widely pitched as solving the problems of 'trust', 'authority' and 'consensus': if it can be mathematically proven that no one in particular has control of the network, then such a network can be used as a neutral, 'trustless' substrate for any potential application, facilitating connections between people, places and things (Nakamoto, 2008; Szabo, 2014; Wood, 2014a; Economist, 2015). More specifically, 'blockchain' describes a linear chain of cryptographically hashed 'blocks' containing information about events. This linear history of events is both stored and verified in a decentralised manner: nodes in the network 'witness' events, and agree on which ones are considered valid through a consensus algorithm and hold the full record of agreed-upon events. This particular aspect, that consensus about events is arrived at algorithmically rather than through some external authority, force, law, doctrine or belief, is what has also lent blockchain the name 'trust machine' and 'truth machine' (Vigna and Casey, 2018). It is a proposition for an algorithmically determined and enforced truth of events that is arrived at without the need to *trust* any person or institution, provably beyond the control of any single part of the system.

The promise of blockchain is that by resolving issues of decentralised consensus and trust, the need for any external mediation disappears, replaced instead by a trustless peer-to-peer network. External mediation refers to any person, institution or authority whether in network engineering, politics, law, finance or economics: a decentralised network would replace authority in which a consensus algorithm resolves any incompatible disputes and ensures consensus in the network; code would replace law and execute immediately and exactly as written; cryptography would ensure the authenticity of records and organise consensus; transactions would take place directly between nodes, circumventing the need for and control by financial institutions; and money creation would be determined by and executed through an immutable protocol rather than a government. This was the basis of the 'disruptive' potential of blockchain and why some have argued that it 'changes everything' (Robinson and Leising, 2015; McKinsey, 2016; Tapscott and Tapscott, 2018). The realisation and development of such a project turned out to be far more complex, and *the political*, in the sense of the possibility for things to be different and the negotiation over such differences, continues to creep back in. Nevertheless, 'blockchain' has managed to capture the

imagination and ongoing efforts of correction and maintenance across a variety of fields, backgrounds, people and places. Rather than immediately dismissing claims made for it, then, with this thesis I aim to 'meet the blockchain halfway' and 'stay with the trouble' (to paraphrase book titles of techno-scientific theorists Barad (2007) and Haraway (2016)) in order to understand how and why blockchain is being developed, maintained and corrected for. The thesis covers the tumultuous and formative early years, focusing on the two largest blockchain networks, namely Bitcoin and Ethereum: I trace the invention of blockchain in the peer-to-peer electronic payment system Bitcoin in 2008, and situate this within a longer history of anti-authoritarian decentralised network technologies; I trace these ideas through the 'generalisation' of blockchain in the launch of Ethereum in 2014, a project to make a 'Turing-complete' protocol, able to facilitate any kind of application beyond currencies; and finally, I discuss two major conflicts in these cases in the years 2016 and 2017 in what has been called a constitutional crisis whereby the main proposition of blockchain, as a decentralised network protocol that would solve the problem of consensus and authority, was severely challenged (cf. TwoBitIdiot, 2017).[1] These crises led to renegotiation of the meaning and purpose of 'decentralisation', the promises of trustlessness and a focus on questions of protocol governance in blockchain systems. Tracing through the specifics of these technical and political histories enables a more precise understanding of the ways in which blockchain as a 'disruptive' technology addresses questions of decentralisation, trust, consensus and authority. With this thesis, I aim to resituate blockchain within a broader politicised history such that its disruptive potential is better understood and its political implications can be more precisely analysed in the literature, as well as deliberately shaped in engineering and development practices.

In this introduction, I first describe the three main ways I address the political in blockchain in what I describe as 'cuts', drawing in particular on philosopher Karen Barad's onto-epistemology (Barad, 2007) and the political theory of Jacques Rancière (Rancière, 2006, 2010), and describe the main research questions that I look to answer. I then describe the broader context and importance of blockchain and the specific cases that I have worked with in the thesis. I finally give an outline of the thesis chapters and its overall structure before concluding.

[1] Turing-completeness describes the ability for a given machine to simulate any 'Turing machine' – usually meaning able to run any potential type of computation. Most programming languages are Turing-complete, but blockchain had up until then been understood as part of a particular application rather than a computational substrate.

1.1 Three 'cuts' on the political in blockchain

The primary research question of this thesis draws together work by theoretical physicist and feminist philosopher Karen Barad and political theorist Jacques Rancière in order to ask *what matters politically in blockchain?* By 'matters', I refer to Barad's understanding of the word as literally *mattering* as in making a material difference (2007, pp.132-185) and by 'politically' and I refer to Rancière's notion of *the political* as the contestation and redistribution of sensibilities (Rancière, 2010, pp. 27–44). The political theory of Rancière describes 'the political' as a moment of disruption and redistribution to a given sensibility. By sensibility, he refers to a common sense understanding of what matters, what is right or wrong, who belongs or doesn't, what is desirable or undesirable and so on. In this sense, the research question addresses the ways that blockchain distributes and redistributes political sensibilities in ways that come to matter also materially. In this thesis I use these two theorists to also answer this question by articulating three approaches to the political in blockchain: the *insensible*, the *sensible* and the *dissensible*. I elaborate on Rancière's conception of the political by articulating my own concept of the *dissensible,* as a disruption to a given sensibility and the question of incompatible sensibilities. I elaborate further, raising the issue of the *insensible,* drawing on work by geographer of the inhuman, Kathryn Yusoff (Yusoff, 2013a), discussing the necessary limits of any given sensibility, of knowledge of what matters, as a problem for the preconditions of the political. Here, I briefly describe the more specific sub-questions of my research that have informed these three approaches.

Bringing together Barad and Rancière in particular allows for an approach to the political in blockchain that crosses material, technical, social, political and economic distinctions. This is the main contribution of the thesis, but it also presents some limitations. Because significant work goes into analysing and shifting the onto-epistemological terms of debate, there is little scope to address the further implications of such a shift. This means that the thesis is primarily focused on epistemological and ontological questions of the two case studies, and perhaps more straightforward analyses of their immediate political implications are not addressed. For example, the different uses of Bitcoin as a currency and payment system or Ethereum as a protocol and platform, and the effects and implications of specific applications, are beyond the immediate scope of this thesis. Instead, the focus is on the protocols themselves, the communities developing blockchain projects, and the ideas, experiences and contexts that inform them as a means to clarify epistemological and ontological understandings of blockchain and shift the terms of critique, debate and development. Three sub-questions guided the research and led to this particular theoretical approach and a focus on the protocols themselves and developer communities, histories and contexts:

1. Which are the active 'mediators' in the blockchain assemblage, what differences do they produce and what political effects do they have? With this question, the aim has been to find out which aspects of 'blockchain' matter in terms of determining the political effects, and therefore also pointing to sites that might be done differently. Blockchain is positioned as a 'disintermediating' technology, meaning eliminating 'mediation' such that, for example, in the case of Bitcoin, transactions take place directly between people rather than via a bank or payments company. One of the primary aims is to get rid of the need for 'trusted third parties', replacing these with a peer-to-peer network protocol. I have taken a critical approach to such claims of 'disintermediation' and instead understand the protocol to be a form of mediation in its own right, organising relationships and determining ways in which such a network might witness, authorise and execute a transaction. And so this question was designed in order to find out the particular forms of mediation taking place through the protocol design. I have also taken a critical perspective on the separation between technical and social concerns, conceptualising blockchain as an 'assemblage' comprising code, hardware, people, promotional material, ideas, technical papers and so on, instead of a coherent technical 'thing'. Retaining a certain openness to what comprises blockchain exactly came to make sense analytically, in particular because of its decentralised nature, where the protocol itself and, for example, what comprises 'Bitcoin' exactly, became contested (see Chapter 6). This research question has been informed by science and technology studies, literature and media theory that conceptualise of infrastructure and technologies as enacting an immanent politics, being an expression and continuous execution and enforcement of a politics in its own right, by shaping a priori what is possible or not and for who (Feenberg, 1999; P. N. Edwards, 2003; Galloway, 2004; Latour, 2005). However, there are aspects of network infrastructures and algorithmic operations that exceed intention, control and full oversight (Seaver, 2014; Burrell, 2015; Amoore, 2016). In order to theorise such aspects, I draw on Yusoff's notion of the *insensible*. This highlights and helps make sense of blockchain as a proposition for a technology initially beyond control by specific authorities, but eventually also humans and human sensibilities more generally (see Chapter 4). The *insensible* then forms the first cut on the political of blockchain.

2. How do the developers and users of blockchain understand, represent and seek to shape the political implications of the technology in terms of decentralisation, trust and consensus? With this question, the aim has been to find out the ideas and assumptions informing the design of blockchain protocols. Concepts and terms such as 'decentralisation', 'consensus' and 'trust' are widely used across different blockchain projects – but it is not always clear whether the concepts are referring to a technical architecture, social conditions or beliefs, or intended effects. This question was in part informed by the idea of translation as employed by N. Katherine Hayles (2005, pp. 89-116), focusing my attention towards qualitative changes that happen in the 'translation of worldviews' when, for example, technological specifications

are rearticulated as socio-political process, or conversely when socio-political ideas are encoded into technical architectures (for example 'decentralisation').[2] But Hayles' notion of translation seemed to imply a more linear, linguistically informed, located and deliberate process than seemed to be happening and so I later shifted this theoretical approach towards Barad's notion of onto-epistemology. Here, concepts are understood as part of assemblages and apparatuses in ways that do not assume a linguistic privilege in determining matters. This has been important in order to make sense of the fact that a given developer's intentions with a specific protocol design does not fully determine how it played out in any simple, linear transfer of idea to materialisation (discussed in Chapter 4). Concepts of decentralisation, trust and consensus would nevertheless in themselves continue to mobilise efforts to build, maintain and correct – such that, for example, engineers, mathematicians and so on develop new consensus algorithms in order to redress centralising tendencies in a given protocol design. This seemed to point to a more general sensibility in blockchain informing a tacit agreement about some overall desirable characteristics and properties that indeed cut across other distinctions between people and projects. Regardless of the confusion or broadness of the use of concepts like decentralisation, trust and consensus, it was clear that these are powerful in mobilising people and efforts to build, maintain and correct for in blockchain. This second question has led to draw the particular cut of the sensible, understood in the sense of Rancière, to form a distinct blockchain sensibility that holds a 'blockchain assemblage' together as a recognisable field despite its broad appeal, explaining more specifically the kinds of 'disruption' proposed.

3. *What are the political differences between blockchain-based developments, and where and how are these expressed? (E.g. in the code itself, in the organisational structure of the developer community, amongst the user-base or elsewhere?)* With this research question, the aim has been to find out the ways in which political differentiation takes place within and amongst blockchain-based projects. My intention has been to trace how and through which forms such differentiation is enacted, with the idea that this might explain firstly what matters politically to different projects, thereby giving an overview of the understandings, theories and politics informing blockchain projects, and secondly the ways that such ideas were being materialised – whether in the code, coding process, the company/organisational structure or deployment or otherwise. This question has been informed by political theory defining the political in terms of the possibility of *dissensus,* (incompatible differences about what matters) and the necessary negotiation and settlement of these drawing on Rancière and Mouffe in particular (Mouffe, 1993, 2005; Rancière, 2006, 2010). These theoretical approaches to the

[2] See also Hayles, 2005, pp. 14-33. Her description of the relationship between digital text, code and what she calls the computational regime as a worldview continued to inform my research and in particular my analysis and writing for Chapter 4.

political have suggested that a suitable strategy for understanding 'the political' in blockchain would be to look for sites of deliberate differentiation, but also, and in particular, moments of disagreement and incompatible positions and the ways in which these are resolved. This final question then led me to articulate the concept of the *dissensible* as the third cut on the political in blockchain, and a way to describe the ongoing potential for incompatible sensibilities to arise.

Through Barad, such questions of the *insensible*, *sensibilities* and the *dissensible* gains material weight and becomes part of how things are made to matter – mattering politically, as well as materially. Barad, theorising at the level of quantum physics experimentation, situates ontological dynamics in relation to sensing apparatuses (Barad, 2007, pp. 97–130). Her *onto-epistemology* describes sensing devices and beings as not only entailing a recognition of some external thing, but in fact is part of determining matters – making determinate what might otherwise be in an indeterminate state of potential (ibid.). She argues that this dynamic takes place by and through all manner of determining sensibilities; that is to say that not only humans determine what matters and how things come to matter (Barad, 2007, pp. 132–186). Barad, then, becomes a means to acknowledge non-human sensibilities in determining matters, such that not only humans are understood to be involved in creating material, nor political realities. This proves effective in particular for approaching the proposition of blockchain as an algorithmic means for determining things, lending some openness to such a proposition, while also giving tools for critically examining it from the perspective that there is nothing necessary, nor inevitable, about algorithmic modes of determination.

1.2 A trustless world: context and cases

Trust, as it is understood in network security engineering, is a bad thing. It means there is a potential vulnerability in the system, an attack vector that can be exploited. For large decentralised networks in particular, the aim is to achieve 'trustlessness', assuming that any aspect of the system might be an adversary. Through Bitcoin and the context of its invention, this understanding of trustlessness took on a broader appeal in popular anti-authoritarian sentiments, before being generalised in Ethereum and giving rise to 'blockchain' as a more general technology that a UK government report described would bring about 'potential explosions of creative potential that catalyse exceptional levels of innovation' (Walport, 2016, p. 4). Here I briefly describe the context in which this thesis has been researched and written and the main cases I draw upon.

Blockchain, as it is understood today, was invented as part of Bitcoin – a proposal for a peer-to-peer digital payment system by the anonymous 'Satoshi Nakamoto'. The project was introduced in a short nine-page whitepaper in 2008 outlining the principles and architecture of the cryptocurrency (Nakamoto, 2008). The idea initially circulated and was developed amongst the subcultural and political contexts of what is called Cypherpunk and cryptoanarchism – formed around the possibility and use of cryptography to radically shift balances of power (Assange *et al.*, 2012).[3] [4] There had been previous attempts at creating internet money that would be beyond the reach of authorities. To mention two relevant precursors: *DigiCash*, a project by cryptographer David Chaum, had been initiated largely because of concerns for the growing significance of the internet for commerce. If an increasing amount of transactions were to take place online, this presented serious privacy issues, the most important of which would be the companies and payment systems that would hold people's records of transactions. This concern is part of the reasoning for peer-to-peer as a type of architecture that would 'disintermediate' such third parties involvement in payments. Another project, *E-Gold,* was more concerned with establishing an online equivalent of gold, with the understanding that this would be a 'superior' form of money. These ideas are also present in Bitcoin and its protocol design, on the basis of eliminating government involvement in money systems. Infamous for being the payment method of preference on the 'Silk Road' online black market, Bitcoin has throughout its history been contentious, initially associated with 'the Darknet' online black markets (Pagliery, 2015), as well as critiqued from a monetary and economic perspective (Golumbia, 2016; Stolfi, 2016; Gerard, 2017), and later associated almost entirely with exchange rate volatility and wild speculative behaviour.

The network and project continued to grow, however, and the rapid highs and lows of its exchange rates only seemed to spark more attention, more media coverage and more interest. The cryptocurrency rose to fame beyond the 'Darknet' and hacker circles in 2011 in what the 'ethical hacker' Denis Jaromil Roio argues were two critical events: the first article in Forbes about Bitcoin, and the use of Bitcoin as a means to donate to whistle-blower project WikiLeaks (Roio, 2013). Major digital payment companies including MasterCard and PayPal had been blocking donations to WikiLeaks following their release of the US military war logs containing evidence of the killing of civilians (Ball, 2011; Matonis, 2012; Roio, 2013; Rizzo, 2014).[5] From early on in its history, Bitcoin has thereby had a real and symbolic presence as a global currency beyond and against the control of governments and global financial institutions, catching the imagination and attention of anyone sceptical of authority. The blockchain protocol distinguishes itself as embodying, on the one hand, a political and

[3] See https://www.activism.net/cypherpunk/manifesto.html
[4] See https://activism.net/cypherpunk/crypto-anarchy.html
[5] See also https://wikileaks.org/Banking-Blockade.html

ideological proposition in its very structure by encoding notions of distributed authority, validation and trust which, on the other hand, are used and implemented for a variety of different political purposes. Bitcoin remains contentious, critiqued on the basis of it facilitating illicit trade (cf. Bradbury, 2014; Martin, 2014; Finklea, 2017), encouraging speculation (cf. Christian, 2014; Farrer, 2018), not being sound money (cf. Mittal, 2012; Lo and Wang, 2014; Constable, 2017), being the cause of scams and fraud (Posner, 2013; McMillan, 2014; O'Brien, 2015), and not being environmentally friendly (cf. Malone and O'Dwyer, 2014; Gabbatiss, 2018). But in the meantime, 'blockchain', a particular aspect of the Bitcoin architecture (sometimes described in the even more broad terms of 'distributed ledger technology') was to become a more palatable technological proposition, bringing about a 'Cambrian explosion of blockchain start-ups' (Robinson and Leising, 2015), with a UK government report going so far as to state that:

> The progress of mankind is marked by the rise of new technologies and the human ingenuity they unlock. In distributed ledger technology, we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation.
>
> – Walport, 2016, p. 4

'Blockchain' became part of several new industries given the names *FinTech* for financial technologies, *RegTech* for technologies in the field of law and *DemTech* for democratic technologies.[6] [7] [8] This shift in attention from 'Bitcoin' and cryptocurrencies as largely Darknet-associated to 'blockchain' as a legitimate technological breakthrough was largely articulated in and through the launch of a project called Ethereum, introduced at a Bitcoin conference by the then 19-year-old founder of Bitcoin Magazine, Vitalik Buterin. The Ethereum project was a project to generalise the blockchain such that instead of verifying and storing transaction data in a decentralised manner, any kind of computation could be held and executed across a decentralised network. The suggested applications would be so-called Smart Contracts (code that would execute automatically in the network), as well as Decentralised Autonomous Organisations (DAO) and Decentralised applications (dApps), discussed in 4.2.1, which had broader appeal for the potential efficiency gains and potential 'RegTech' applications.

A trustless architecture in terms of information security practices entails a secure architecture, whereby no single aspect is entirely depended upon. Ethereum, in generalising the Bitcoin

[6] FinTech, see for example https://www.pwc.com/sg/en/publications/fintech-apac-landscape-devt.html and https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/502995/UK_FinTech_-_On_the_cutting_edge_-_Full_Report.pdf

[7] RegTech, see for example https://complyadvantage.com/blog/what-is-regtech/ and https://www.techworld.com/picture-gallery/startups/uk-regtech-startups-watch-3648554/ and https://www.ibm.com/blogs/insights-on-business/banking/blockchain-kyc-game-changing-regtech-innovation/

[8] DemTech, see for example https://demtech.io/ and https://demtechvoting.com/ and https://demtech.chathamhouse.org/ and https://dcentproject.eu/

architecture, also generalised the question of trust and trustlessness, from its explicitly anti-authoritarian context in Bitcoin to a broader question in business, finance and politics. Cryptographic proofs became a solution to the 'trust' problem for any context or situation – and blockchain, from its pre-history in decentralised network technologies seeking to defeat authorities, became a 'disruptive' technology on the basis of automation and potential efficiency gains. In this thesis, I argue that there are significant issues, technically, politically and socially when 'trust' as a problem is generalised, whereby much of the purpose of blockchain loses its meaning. With this thesis, I aim to rearticulate some of the disruptive potential of blockchain that goes beyond efficiency gains and resituate blockchain in a more politicised history. By doing so, the specific applications, attraction and political significance of blockchain are also clarified.

Blockchain, in the meantime, continued to find interest amongst explicitly anti-authoritarian political contexts. It is worth briefly describing a third case study which over the course of my data analysis receded to the background, but which nevertheless has informed much of the context of this study. Bitcoin and blockchain were being developed also during a time of large decentralised social movements across North Africa in the *Arab Spring*, Europe in the movement of the squares in Spain, Greece and Portugal and *Occupy* in the US (cf. Gutiérrez-rubí, 2011; Alcazan *et al.*, 2012; Gerbaudo, 2017). Emerging in this geo-political context, the Bitcoin protocol started to be framed as addressing the lack of trust in existing financial and governance institutions – not by repairing legitimacy, but by creating a system that works regardless of and despite malicious intent by any actor. In other words, a 'trustless system', designed for a trustless world. At the time, there were experiments amongst social movements for creating new social currencies, a particularly ambitious one is Faircoin, a project to develop a cryptocurrency for the global cooperative movement, which made out a third case study during my empirical research. Faircoin was started by the Spanish anarchist, Enric Duran. In 2013, Duran left Spain after being bailed out of prison, having taken out loans in banks across Catalonia totalling about €500.000. He declared publicly that he would not repay the loans and instead used the money to support cooperatives and anarchist projects in the region and set up what is called *Faircoop* – an organisational vehicle to expand existing networks of cooperatives in Catalonia to an international scale. The movement employed what they called 'tax-disobedience' strategies and aimed at an exit from existing financial and political structures by building new ones in their place. Faircoin would be 'the first democratic and assembly-based cryptocurrency', and would facilitate exchange in the network as it grew globally.[9] Faircoin was a 'fork' of Bitcoin, drawing on but significantly modifying aspects of its code. The attraction from an anarchist perspective was the possibility of scaling otherwise locally bound social currency projects. As a cryptocurrency, Faircoin is a fascinating

[9] Quote from an interview with Sebas, a Faircoin developer, in Girona, November 2016.

proposition because it operates with the inverse security assumptions of Bitcoin and Ethereum: Faircoin as a technical architecture heavily relies on building social trust while Bitcoin and Ethereum are designed to operate under conditions in which anyone might be an adversary.

In selecting Faircoin as a case study, I sought comparative insights that would allow me to analyse which aspects of cryptocurrency protocol designs were considered to matter and how these were coded differently with different politics in mind. In this sense, Faircoin was a useful comparative case in order to better understand the specificity of Bitcoin and Ethereum and the sensibilities that informed their design. However, as a case on its own, Faircoin brought up very different theoretical questions than those raised by Bitcoin and Ethereum, and has therefore not been treated in any significant manner in the thesis. This is equally true for other significant projects, such as Holochain, that deliberately encode a different political intention and ethos, but which are beyond the immediate scope of the thesis. I explain this in more depth in Chapter 3 where I describe my methods. It is the hope, nevertheless, that by rescuing and articulating a more specific history and context of Bitcoin and blockchain, and reground the conditions of debate, that such projects also will benefit from such clarification.

1.3 Outline of the thesis

Here I briefly describe the overall structure of the thesis and contributions made in each of the three 'cuts'. After introducing blockchain and describing the broader reasoning and context for this thesis in this chapter, in the next, Chapter 2, I lay out the theoretical foundation for the thesis in more detail, introducing Barad's *onto-epistemology* and discuss its merits as a basis for research on blockchain. I describe the theories and thinking informing the three 'cuts' I have taken in this thesis, discussing each in relation to debates in the literature. The debates that I address have a relatively wide range, from new materialism and animism to platform economics and political theory, so I briefly describe how and why I draw from such disparate sources and discuss the merits of doing so. In Chapter 3 I describe and discuss the research methods and methodologies that I have employed in doing this research. The chapter introduces the research design and cases, the reasons for selecting these as well as the reasoning behind a case study approach. I discuss my positionality in the field and ethical issues arising from this particular research and positioning as a 'critical insider' in the field. I then describe the research phases and data gathering and the ways in which I went about analysing the data, and the limitations and scope of my particular methodological approach.

Apart from the extensive theoretical discussion in Chapter 2, Chapters 4, 5 and 6 form the main body of the thesis and comprise three empirical chapters that are shaped by my three 'cuts' in the field. Each of these is structured in a similar manner: I first introduce the chapter and the particular 'cut' to questions of the political. I then address aspects of the Bitcoin case study in the first half and the particular understanding of 'blockchain' that comes to matter through this cut. In the second half of the chapter I address aspects of the Ethereum case study as a generalisation of blockchain and the implications of that particular cut. Each of the chapters therefore addresses both case studies, approaching them through the *insensible*, *sensibilities* and the *dissensible*.

The main contribution of Chapter 4, titled *A politics for the insensible,* is to articulate and address the question limitations of a blockchain mode of determining trust and consensus. I do this firstly through a clarification of the very specific ways that 'consensus' is arrived at in Bitcoin through an arrangement of cryptographic proofs. The chapter in this sense looks to make specific what is otherwise framed in general terms, namely concepts of decentralisation, trust, consensus and autonomy. I aim to describe the very particular ways that 'consensus' is understood and achieved in blockchain, through what is called 'proof-of-work' and other rules that form the consensus algorithm. I do this in order to be able to discuss how Bitcoin was suggested to have solved the problem of trust by introducing a decentralised architecture based on cryptography proofs. Because the architecture is based on cryptographic proof rather than needing to trust someone, it is claimed to be 'trustless'. Through this discussion of the Bitcoin protocol, the main aim and achievement is to trace through these claims of trustlessness, and point to their precise limitations, such that it can be made clear for who and what exactly such an architecture can be understood as trustless. The second half of the chapter describes the Ethereum protocol and the ways in which it generalises the Bitcoin architecture, both in terms of the kind of data stored in the blockchain, but also the creation of value tokens as a means to coordinate computational resources. I then discuss the specifics of generalizing the conceptualisation of trust, and how it has informed the development of types of applications determined through algorithms designed to be beyond the control of humans. Here, I articulate limits to algorithmic modes of determinacy on the basis of Barad's notions of multiple forms of determinacy (Barad, 2007, pp. 132-185) and Yusoff's notion of the insensible (2014a). The contribution here is to shift the ground of debate and add to the literature that suggests that algorithmic forms of determinacy can be critically addressed without necessarily having to assume or reassert complete control or knowledge by humans (Kitchin, 2014; Seaver, 2014; Burrell, 2015; Amoore, 2016; Amoore and Raley, 2017). It therefore presents a useful ground from which to critically discuss blockchain and algorithms that does not immediately construct a competition for control between humans and machines.

The main contribution of Chapter 5, titled *Blockchain sensibilities*, is to articulate the specific sensibilities that hold the blockchain assemblage together and their specific pre-Bitcoin provenance in the political histories of network technologies. Explaining why and from where decentralised network projects came, the specific form of anti-authoritarianism that informs the sensibilities can be foregrounded, which also suggests a slightly different angle from which to understand the 'disruptive' potential of blockchain. I draw out this history to address, in particular, criticisms of blockchain as reproducing the logics of capitalism. I do not negate these, but draw on Gibson-Graham's diverse economies approach (Gibson-Graham, 2008) to open up a space that exceeds questions of capitalism. By doing so, I articulate the specific computational affiliations of a blockchain sensibility which also point to the ways in which in particular Ethereum seeks to become a general platform for *any* potential economic, political or social system. By placing blockchain in the politicised histories of decentralised network technology rather than in and only in relation to questions of capitalism, the thesis suggests redrawing the political map of blockchain. This repositioning turns out to be hugely informative for understanding the particular aims and intentions of blockchain, in particular the attraction of developing code (Smart Contracts) and types of organisations (Decentralised Autonomous Organisations) that are beyond control. The concerns, I argue, pertain primarily to questions and concerns of network computation and information security practices, the aim being developing systems that cannot be targeted, controlled and shut down by any authority. In this sense, I am to draw out a ground from which to address the merits of blockchain that are not immediately concerned by and that exceed questions of capitalism as a way to carve out some forgotten political space.

The main contribution of Chapter 6, titled *Dissensible matters*, is to discuss the ways in which incompatible differences are resolved in and around a technology that was supposed to have solved consensus. I do this by tracing two major conflicts in Bitcoin and Ethereum. The so-called *Bitcoin scaling conflict* was a conflict over a technical issue of how to scale the Bitcoin network without compromising on decentralisation. The conflict brought to the foreground the ways in which protocols are or should be managed in a decentralised system, raising questions of balances of power across different actors and causing significant discussions about protocol governance and scaling that were to last several years. The *Ethereum DAO exploit* was a hack of the first explicit attempt at developing a Decentralised Autonomous Organisation (DAO) that would be controlled purely on the basis of its Smart Contract code and be beyond human control. A hacker exploited part of the contract code to siphon off large amounts of Ethereum cryptocurrency, ether, causing the Ethereum Foundation to enact what is called a 'fork' in the code – essentially creating a new version of Ethereum and records of events in which the hack had not taken place. This caused significant debate about the purpose of decentralised systems and the promise of trustlessness. In this chapter, I introduce the concept of the dissensible, suggesting that dissensus is never finally resolved;

its negotiation merely changes character. Such changes to the ways in which dissensus is resolved nevertheless *matter,* however, because they determine who or what has the capacity to take part in determining how dissensus is negotiated and resolved.

The chapters are to some extent chronological in the sense that Chapter 4 discusses some of the pre-Bitcoin history of peer-to-peer in the '90s and early '00s, Chapter 5 addresses some of the determinacy that characterised the early years of blockchain in the years 2008 to 2016 while explaining the protocols and the ways in which this determinacy is encoded, and Chapter 6 describes two major crisis that caused rearticulations of such a determinacy in the years 2016 and 2017 and opened up the industry and efforts towards more sophisticated understandings of consensus protocols and the political.

Finally, in the concluding Chapter 7, I recap and reflect on the main contributions of each of the three onto-epistemological 'cuts' that I articulated and worked with in Chapters 4, 5 and 6. I outline the limitations of these approaches and further research that they open up. I also pick up on and discuss a thread that carries through each of these three main chapters, namely the question of limits, edges and relationships. If cryptographic proofs can determine trust in a given piece of data and decentralised network, it invites the question of the precise limits of such trust, what happens beyond its edges and how such a form of determinacy relates to other ways of determining things.

The *Disassembling the Trust Machine* thesis is driven by the question of what matters politically in blockchain technology. The aim is to shift the preconditions of debate about the proposed disruption by blockchain for 'legacy systems'.[10] Blockchain technology is in part a proposal to resolve 'the political' through technical means: decentralised networks to solve the problem of authority; cryptography to solve the problem of systems integrity; game theory and incentive design to solve the problem of security and malicious behaviour. Involving political and economic dynamics in the protocol design has also opened up computational systems to political and economic dynamics. Without further ado, the in next chapter I describe the theoretical tools I have developed in order to disassemble the blockchain 'trust machine' and reassemble it again in three different ways.

[10] In discussion with people in blockchain contexts, political, legal and financial systems are often referred to as 'legacy systems'.

2 The insensible, sensible and dissensible

When you step into the conversation about the political in relation to blockchain, you're hit by a cacophony of claims, concerns, hopes, sales pitches and opinions. Excitement and worry ripple through the conversation, and it's tricky to not immediately 'take sides' in determining its political implications. This is because blockchain, as a proposition, is often treated as a coherent thing, while at the same time its determination and boundaries are in themselves highly politicised questions. My intention with this PhD project is to suspend judgment, and instead observe and describe these debates as part of an ongoing process of articulating the political significance and implicit politics of 'blockchain'. I therefore consider these very debates as to the definition and implications of blockchain to have political implications in their own right (as also noted by Golumbia, 2016; Reijers & Coeckelbergh, 2016), and will look closely at how these form part of a political reasoning, inform the technical materialisation of blockchain and shape the development process.

Bitcoin was a proposal to solve a problem of 'authority' and 'consensus', as articulated and addressed through the specific and particular form it takes in computer network information systems. Very quickly, and as the remit and project was expanded from payment systems and cryptocurrencies to the blockchain and databases and computation more generally, the Bitcoin consensus mechanism appeared to offer a solution to problems of authority in potentially *any* field or industry. And so a body of popular literature emerged, describing blockchain as a radical disruption and transformation of all aspects of governance, money, economics and politics (cf. Swan 2015; Tapscott & Tapscott 2018; Filippi & Wright 2015; Vigna & Casey 2018). The challenge is how to think of *the political* in relation to a technology that claims to solve it – while also being attentive to how such a proposition nevertheless becomes real in the sense of mobilising and materialising efforts, even as these materialisations never fully correspond to the proposition. In order to do this, a theoretical approach is needed that can assist in tracing and articulating how 'blockchain' is determined in different ways and the political aspects of this determination.

How things come to matter, in the sense of becoming determined as material things as well as in the political and ethical sense of having importance, are two of the main questions raised and articulated by the philosopher Barad in her onto-epistemology '*agential realism'* (Barad, 2007, pp. 132–185). Using Barad's approach as well as her conceptual vocabulary throughout this PhD then brings to the foreground the question of determination as a political

and ethical question. Perhaps even more crucially, Barad's onto-epistemology does not presume that determination is solely in the hands of humans, but instead positions processes of determination through a quantum physics perspective as an ongoing dynamic of materialisation across any scale, materiality or lifeform (Barad, 2007, pp. 247–353). Such an approach lends a certain openness to some of the propositions and hopes for blockchain, namely by involving non-human dynamics (in this case maths, network computation and so on) into what have previously been considered the solely human domains of politics, economics and law. Conversely, her approach is also helpful for broadening the scope of what is understood to constitute 'blockchain' to include human, social and other dynamics. This is important exactly because claims made of blockchain are so heavily based on assumptions of a purely objective technical realm that exists separately from what are perceived as necessarily subjective humans. The political can be sensed through and in different aspects that form 'blockchain' at different times and places, not only as a technology but also as a set of ideas, headlines, whitepapers, promotional material, developer cultures and so on. Because the idea of 'blockchain' is a hook for different and contested agendas, and because it proposes a radical reconfiguration of the political, neither 'blockchain' itself nor its political significance should be fully pre-assumed from the outset. Instead, its articulation as political is the primary question and endeavour of this thesis.

In this chapter I set out the theoretical approaches, debates and concepts, drawn on in Chapters 4-6, that I employ in order to articulate and clarify political dynamics in 'blockchain'. I complement Barad's onto-epistemology with an understanding of *the political* that I draw from political theorist Jacques Rancière, namely as a moment of a disruption and redistribution of 'the sensible' (Rancière, 2006, 2010). The combination of Barad and Rancière's thinking allowed me to draw three 'cuts' in the field, addressing the question of what matters politically in blockchain from three different angles, namely the *insensible*, the *sensible* and the *dissensible*. I discuss each of these in relation to a rather diverse set of debates, as will become clear below, ranging from animism to platform economics. This broad range is the result of, and is hopefully justified by, a methodology that relied almost exclusively on my research questions, which meant that I crossed a number of fields and debates while seeking their answers. This broad range of debates is also shaped by adopting Barad as a means for overcoming technological and human determinisms, which does open up my research question to possible answers from fields that address the political, the non-human and the technical as well as the economic. Instead, by allowing my research questions to guide this methodology, a certain rigorous thread has nevertheless been maintained. This chapter, and the thesis more broadly, should therefore be read as outlining three possible ways in which the political might be addressed as a question of blockchain, rather than offering an exhaustive review of their related literature and debates. Instead, the focus remains on how to approach the political in blockchain; this thesis forms an exploration of this.

Addressing the political through the notion of 'sensibilities' rather than through explicit opinions, theories and ideology opens up a much broader theoretical field. It means that *the political* as a potential for disruption, a moment of 'dissensus', is relevant for and can occur in and through any potential contexts, materialities and debates, including, in the case of blockchain, questions of 'network attack vectors' or debates about 'blocksize' in the Bitcoin blockchain and so on. It also raises the question of the insensible – that which has not yet been included or is simply beyond a given sensibility – and the challenge of how and whether to make the 'insensible' matter politically. These different approaches to *the political* imply different 'cuts' that include and exclude elements as comprising the very thing called 'blockchain'. I use the word 'cut' from Barad in reference to her explanation of onto-epistemological cuts whereby phenomena are made determinate by drawing a cut through an otherwise indeterminate field (Barad, 2007, p. 148). And this thesis indeed is intended to contribute to determining the political possibilities and significance of blockchain. This chapter is structured as follows: I will first briefly introduce Barad's onto-epistemology, known as agential realism. I will then articulate the *insensible* in relation to 'blockchain' as an instantiated technology and protocol, addressing its determinate claims. Here, I suggest a politics for the *insensible*, drawing on work by geographer of the inhuman, Yusoff (2013b) as a way to address that which is beyond a particular sensibility. The insensible might refer both to behaviours of blockchain, algorithmic and network systems, as well as forms of life and matter that are beyond the sensibilities and determination of such systems. I discuss ways of articulating and addressing the insensible, drawing on new materialism debates and animism.

I then articulate the *sensible* as a theoretical cut on the field, whereby 'blockchain' describes a certain sensibility that informs projects and protocol development, regardless of the extent to which these manage to live up to such a sensibility. It nevertheless matters as an understanding of blockchain that shapes new projects, maintenance and corrections in efforts to materialise this 'blockchain'. Here, I draw on the political as a reconfiguration of what matters and is made *sensible*, drawing on Rancière's notion of the political as a 'redistribution of the sensible' (2010, pp. 27-44), where, in Baradian terms, new things emerge as mattering. Drawing on what Gibson-Graham introduce as *diverse economies* (2008), this approach then looks at how these new sensibilities emerge in relation to other political (and economic) spaces.

In the last section of the chapter, I articulate the *dissensible*, as the ongoing possibility for things to be different, and for such differences to be incompatible. Here, I draw on primarily political theorists Mouffe (2005) and Rancière (2010, 2006) in order to focus on the particular ways in which the dissensible is negotiated and managed. Such incompatibility either necessitates an expansion and redistribution of the sensible or another way to accommodate for the dissensible – in relation to and through a technology that was supposed to have solved

dissensus. Where the protocol was supposed to solve the political, in turn the management of the protocol became politicised, and code repositories became a vocabulary for modes of governance. The next chapter will then describe my methods and how I arrived at these approaches through my empirical research.

2.1 Meeting the blockchain halfway

The intention in this thesis was to 'meet the blockchain halfway' by following claims made of blockchain through to their historical and technical sources in order to understand how it came to be as a political proposition, why and how claims made of it matters, how they are sought to be encoded and enacted, and how they play out, addressing the political in each of these moments. The challenge is to find perspectives of *the political* that can speak to or at least recognise the non-human as mattering, because a major aspect of blockchain is to draw in and involve non-human cryptographic and algorithmic processes and dynamics in determining and executing the political. A second and related challenge was to find perspectives that would not be entirely seduced nor frightened by such a mathematical and computational conversation, but instead would be able to listen and look at the world as described and determined by these. This required an epistemology, and indeed ontology, that would allow for a rigorous tracing of political dynamics but also suggest some resolution to, and ways of making sense of, social or technological determinisms. This became only more urgent as the empirical research progressed, making increasingly clear that decentralised systems make such questions of social and technological determination even more complex (meant in terms of complexity, not just 'complicated'). This entails shifting the ground of debate away from the question of whether 'the technical' or 'the social' is a more appropriate means to resolve the political, and instead focusing on how assemblages, which include technical, social and other elements, come together to enact a given condition – or fall apart under other circumstances. Here, the relational is foregrounded as ontologically determining, in that relations are what shape the characteristics of a given assemblage rather than being predetermined.

In this section I discuss and define some of the main concepts used in Barad's onto-epistemology (Barad, 2007), which have significantly contributed to my work tracing what matters politically in blockchain: re-grounding of the concept of objectivity; apparatuses as material-discursive; techno-scientific practices as performing a 'cut'; the ethical and political implications of a 'cut' as onto-epistemological; a 'cut' as ontologically determining 'phenomena'; phenomena as 'entangled'; and these onto-epistemological cuts as not necessarily enacted by a deliberate agency of humans but as entangled quantum states.

2.1.1 Onto-epistemological approaches

In her onto-epistemology Barad draws in epistemological work and conceptual developments as part of an ongoing, never final ontological process in what she calls *agential realism* (Barad, 2007, pp. 132–185). Onto-epistemology and the foregrounding of the relational aspect of ontological processes of becoming is not a unique contribution from Barad (cf. Appadurai, 2015; Bennett, 2010; DeLanda, 2004; Haraway, 1992; Latour, 1992; Papadopoulos, 2011; Strathern, 1996). As part of what has been discussed more broadly as an 'ontological turn', such approaches argue that descriptions, language and the social should be understood as part of materialising how the world evolves, unfolds and becomes. Onto-epistemological approaches do not assume that 'things' have innate essences, instead focusing on how a given thing becomes and is determined, also materially, in relation to and by other phenomena. The attraction of Barad in this case is that she takes as her starting point techno-scientific practices, and does so in a way that is coherent with the epistemological approaches of these practices rather than taking them as object of observations. Her onto-epistemological approach therefore lies in the possibility of meeting such practice – in this case blockchain development, computer engineering and cryptographic research – 'halfway' and being involved in shaping them.

Blockchain has been proposed as a technical solution to socio-political dynamics, based on the premise that as a technical apparatus it is neutral, objective and separate from the socio-political whims of humans and 'messiness' of the world. And yet, as described and discussed in chapters 4-6, 'the blockchain' cannot be so easily extracted from the world, nor from the humans that code and use the systems. How then to understand the relationship between an objective world, the mathematics and technical architecture that form the blockchain and subjective opinions, perspectives and behaviour? Barad addresses the tendency to divide 'the objective' from 'the subjective' head on through the work of quantum physicist Niels Bohr (Barad, 2007, pp. 118-131 and pp. 153-155). Rather than understanding the objective as a fixed material exterior reality, which we in our limited subjective interiors attempt to understand by probing with scientific apparatuses, Barad situates such probing, sensing and describing as material-discursive practices that are *part of*, not separate from, the making and remaking of material reality.

Barad takes as her explanatory starting point the famous wave-particle duality in quantum physics, whereby one experimental arrangement measures light as a particle and another as a wave. She draws on Bohr's explanation of this contradictory state of affairs; that this is evidence that the characteristics of light are indeterminate until and unless they are met with a given measuring device, which at that point determines a phenomenon with a set of characteristics (Barad, 2007, pp. 97–130). Rather than the device measuring some *intrinsic*

nature of light, the relation between the measuring device and light determines a given phenomenon – for example, determining light as either particle or wave. What this means, argues Barad is that the measuring apparatus is itself part of an ontological process of determining and materialising a given phenomenon (ibid.).

The apparatus is not a neutral measure of an objective exterior but is implicated and matters, literally, by making what she calls an *agential realist 'cut'* in an otherwise indeterminate field, and taking part in determining a phenomenon with distinct characteristics. Barad is careful to state that not every arrangement will be effective. Not every apparatus will simply materialise new realities at the whims of an engineer or scientist, and she explains this by drawing in the non-human as active in the given arrangement rather than as mute matter to be manipulated. This is also how she explains that some things 'work' and others don't, regardless of an individual person's will or opinion (Barad, 2007, pp. 167-175).[11] The material and non-human both have a presence, a way of being that needs to be worked with effectively in order for a given apparatus to be successful and effective. The notion of objectivity is then re-grounded here as the ability to accurately describe the set of conditions and arrangement that would be able to reproduce and determine the same phenomena. Rather than describing a fixed, pre-existing reality, then, Barad, via Niels Bohr, defines 'objectivity' as the ability to accurately describe the conditions that would produce and materialise some phenomena such that it can be reproduced. Importantly, and in a significant leap from Bohr's explanation of a laboratory situation, the material-discursive apparatus in Barad's thinking is expanded to a meta (quantum)physics, whereby *any* observing agency might enact an agential realist cut in a field of ontological indeterminacy. Agential realist cuts are enacted through all kinds of human and non-human entanglements – not only in the laboratory or by humans. The ethical and political implications of this shift in definition for blockchain are significant: rather than existing as an objective 'truth-machine' exterior to human, historical and socio-political dynamics, 'blockchain' is comprised of a collaboration between a vast array of materials, thinkers, notebooks, experiences, institutions and concepts, like 'decentralisation', and so on that come together to materialise a new set of conditions, literally shaping what matters.

The agential realist cut in an otherwise indeterminate field entails exclusions; when light is determined as a particle, its potential to be a wave is excluded. This determines a different state for light, and more broadly a process of ontological differentiation. The construction of such onto-epistemological apparatuses and the 'cuts' that they perform are therefore deeply ethical and political, less because of who enacts them and with what intention and more because they literally matter and are part of materialising reality. This raises the questions of

[11] STS literature has also articulated and problematised the question of what it means that something 'works', describing how such a concept as well as our current understanding of for example efficiency and so on is also contingent on historical, cultural, social and political contexts.

'... how different differences get made, what gets excluded, and how those exclusions matter' (Barad, 2007, p. 29) and demands a careful attentiveness to such practices.

> ...attending to the complex material conditions needed to specify "intentions" in a meaningful way prevents us from assuming that "intentions" are (1) pre-existing states of mind (2) properly assigned to individuals. Perhaps intentionality might be better understood as attributable to specific sets of material conditions that exceed the traditional notion of the individual. Or perhaps it is less that there is an assemblage of agents than there is an entangled state of agencies.
>
> – Barad, 2007, p. 23

The difficulty of the agential realist approach is therefore that it refutes any possibility of definitively assigning intention or agency (and therefore ethical and political responsibility) as belonging to any given individual, institution or system, whether human or non-human, instead directing attention towards tracing and carefully unpacking the ways in which phenomena become determinate in each and every entangled case. Though extra work is then required when making use of an onto-epistemological approach that does not assume neatly organised agencies, its use allows us to understand the potential for complex distribution of agencies, enactment and enforcement that are operationalised in and through 'blockchain'.

Understanding blockchain as assemblages, and through Barad's notion of entanglements, helps articulate more precise questions about what matters in shaping the political significance of it rather than assuming this already whether in socio-political contexts or mathematical purity. Analysing blockchain as assemblages therefore makes it possible to ask more specifically what exactly comprises the blockchain assemblage, and how and by who it is determined. What is excluded in this determination? How does the assemblage deal with mutually exclusive positions? What holds the assemblage together over time and how does it develop? These questions are pertinent for any analysis of blockchain exactly because, for example, even the delineation of what and who exactly comprises 'Bitcoin' turns out to be politically significant and indeed contested/contestable (see Chapter 6). The running concern of this thesis is thus Barad's agential realist 'cut'; determining the matter of blockchain; what does or does not matter politically; and tracing clues across cultures, beings, materials and contexts in order to understand who, how, and why things are determined the way they are. This is, in turn, also the task of the thesis itself: to offer up another set of 'cuts' in the as yet indeterminate aspects of blockchain as a political phenomenon. In Baradian terms, the three approaches to the political pursued in the thesis then can be stated firstly, in terms of the

insensible, and the question of an ethics and politics that is aware of the exclusion also performed in the cut; secondly, in terms of the *sensible*, whereby the cut literally remakes (redistributes) the *sensible*; and finally, in terms of the resolution of the *dissensible*, whereby mutually exclusive onto-epistemological positions are negotiated.

Throughout the thesis, I employ concepts and understandings from Barad's ontoepistemology in relation to other theorists of the political, and explaining these as I go along. To conclude this overview of Barad's contribution, it is important to note a few limitations to such a Baradian approach. By drawing in the non-human and questions of quantum entanglements, there is a risk of losing sight of the people, places and situations that are part of determining a matter. To put it differently, if agency and intentionality is from the outset presumed to no longer rest in a specific decision-maker, person, institution or otherwise, such moments of decision, where things indeed are determined, can easily be overlooked. It is essential therefore that the employment of Barad's theoretical approach does not lead to abstractions whereby specific things, people, places and so on are not considered to matter because they are not sole 'possessors' of agency. Rather the opposite: exactly because one cannot presume that agency and intentionality necessarily and always lies with a given person or institution or device, one needs to pay extra attention to the detail in such moments in order to understand who or what is part of enacting a 'cut', of determining a matter.[12]

2.2 The insensible

The following section turns to the question of how 'blockchain' is materialised and enacted in and through whitepapers, protocols and computer networks as an immanent and continuously executing politics. The political as a redistribution of the sensible is challenged here in terms of the limits of the sensible. The insensible suggests limits to what can be sensed and determined through blockchain protocols; a haunting awareness of that which exceeds the sensible. It raises the questions of what exactly can be known about the immanent politics of protocols as they interact with large network infrastructures, and whether is it possible to be ethically and politically responsible towards *the insensible* in the design and deployment of deterministic blockchain systems. This section looks at questions regarding what can be known about the matter of blockchain as a material, technical system first by discussing the

[12] Another assumption that should be highlighted here is that when I use Barad's concepts in this thesis I assume that the quantum-scale insights that are at the basis of her ontoepistemology can indeed be extrapolated to other scales. However, because using Baradian concepts proved pertinent for developing a different understanding of the ethical and political in relation to blockchain, I decided to proceed and work with this assumption.

determinate claims of blockchain protocols and their limits. Secondly, by drawing on literature from what has been called new materialism debates, in particular in relation to non-human agency, questions of control are addressed from the perspective of material agencies.

2.2.1 Determinate and emergent

> if the insensible alerts us to the work of sense in securing the bringing into relation, its configurations, and its *a priori* orientations, then it also points towards modes of exclusion and forms of resistance in our thinking with non-human others
>
> – Yusoff, 2013a, p. 224

> Dealings in this proposed system would have several attributes not often found in the real world. The incorruptibility of judgment, often difficult to find, comes naturally from a disinterested algorithmic interpreter.
>
> – Wood, 2014a, p. 1

The promise of the 'disinterested algorithmic interpreter' that Ethereum developer Wood describes above in an early technical paper outlining the Ethereum project is a proposition to determine relations in a manner and through a mode that is non-human. The algorithmic interpreter here is a promise of complete control, as an incorruptible system, the legitimacy of which is, at the same time, premised on it being beyond control (by any single human). *The insensible* raises questions of limits to the political that is both internal and external to such claims of a disinterested algorithmic interpreter. A politics of *the insensible* is to raise the question of how to take into consideration that which cannot, has not yet or will never be made sensible in a given registry; a haunting awareness of ways of reasoning and events that exceed human comprehension both internally in complex networked and algorithmic systems as well as externally amongst lifeforms and things that never will enter into contact with such algorithmic modes of determination. If the political comes to matter through a disruption of a given sensibility, the insensible raises the question of before or beyond the political; that which might never directly make its self matter to our sensibilities and sensing apparatuses.

The issue of response/responsibility towards the insensible is raised by geographer of the inhuman, Yusoff, in the context of loss of biodiversity and the awareness of mass extinctions of forms of life that have not been and never will be known or registered: '…that which is strange, nonintuitive, insensible—that which is remote from human comprehension or intelligibility—like phytoplankton, seeds, fungi, geological epochs, or multi-celled organisms at the beginnings of time' (Yusoff, 2013a, p. 225). But the concerns she raises are not about constructing a sentiment or sensibility to imagined 'micro/macro limit experience at the chapel

of extreme environmentalism' (ibid.), but are designed to raise a broader question about how we (don't) relate to that which is at the limits of or simply never will be sensed, whether mineral, biological and including technological or otherwise. The insensible makes itself felt here in two ways: as an awareness of the limits of the protocol in taking into account and being able to determine all that matters, given that what matters might be beyond and may never enter the realm of the *sensible*; and as the possibility that this algorithmic interpreter itself, as a networked system that interacts with other systems, might be beyond the immediate visibility, comprehension and sensibilities of humans. Although what matters, along with certain intentions, values and concepts, will inform a given technology, they do not fully determine the effects. The 'blockchain' that suggests itself for political analysis through this second set of debates is the realm that tends to be understood as the purely technical one, articulated in whitepapers, code GitHub repositories, hardware and other traces of the technical.

Determinacy

The aim of resolving the political through a disinterested algorithmic interpreter stems from ideas of humans and human language as biased, flawed and vague, whereas the languages of mathematics and code are understood as pure in that they express universal principles and execute as written rather than through unpredictable interpretation: code not only describes, it simultaneously executes (Galloway, 2004; Hayles, 2005).[13] The Ethereum blockchain is described by Wood in the technical paper as 'a system such that users can be guaranteed that no matter with which other individuals, systems or organisations they interact, they can do so with absolute confidence in the possible outcomes and how those outcomes might come about.' (Wood, 2014a, p. 1) It is a project to establish a layer of determinate relations that, regardless of who, what or where, will execute as written. This is described as constructing a neutral outside or beyond 'the real world' (see quote above), a layer in which disinterested execution comes 'naturally'. Claims of such technical, otherworldly or mathematical neutrality can be unpacked in several ways drawing on different strands of Science and Technology Studies literature (STS). Instead of assuming that technology exists and executes along objective and pure pathways that are autonomous and beyond the will of necessarily subjective humans, STS literature situates the forms that technologies and infrastructures take as emerging from and as part of a broader set of conditions. This includes social dynamics (Callon, Law and Rip, 1986; Star, 1999; Latour, 2005), historical contexts (Daston and Galison, 1992) and as expression of political and cultural struggles that in turn determine which development pathways are chosen (Feenberg, 1992; P. N. Edwards, 2003). Importantly, social and political concerns are articulated as being the very reason and

[13] Even if we understand language as performative rather than representational, it performs in a multitude of ways, predicted and unpredicted, while code executes a more limited, predefined set of functions.

conditions for how a given technology or infrastructure emerges and develops in the particular ways that it does.

If technology were a form of material politics, an ongoing silent enforcement of a given order, then disentangling the political and ethical ideas that have been the basis for the technology would reveal its politics. Tracing the theories along with the social, political, economic and cultural contexts that inform a given protocol then would also open up the possibility of political differentiation by deliberately introducing a different set of theories and contexts to inform what is encoded and enacted. However, such deliberate political differentiation still assumes technological determinacy in the sense of determining a different set of ideas in and through the protocol. The promise of determinacy has its own impetus towards articulating ever more in and through the protocol in order to determine and control more and more effects. Determinate systems seem to offer the ability to determine effects, and the temptation to harness such infrastructures 'for good' by encoding a different set of politics into them. And yet it is unclear, especially in complex networks systems, how much can be deliberately determined through a protocol.

If a protocol can be considered an encoding and continuous execution of a given distribution of the sensible, then the political plays out in terms of encoding a different sensibility. The blockchain protocol determines transactions, relations and agreements, and promises a disinterested, continuous execution of such determinate conditions. The problem with determinacy is not only about whether the right ideas have gone into its construction, but also about the need to determine ever more things through a particular determining apparatus in order to establish and secure a given order of things. This raises some initial questions the regarding the limits of protocological determination, in the sense of what and how much can or should be determined through these. In the context of blockchain and IoT for example, to what degree should such infrastructures be embedded into things, people and places, and what kinds of situations (political, economic, legal, religious, emotional etc.) can be determined through them?

Already the question of limitations or edges is of concern in the information security community; a secure protocol is meaningless if the security conditions of interactions with the protocol by different actors are not addressed and taken care of. What this reveals is that a protocol can be trustless and yet require plenty of trust. A few authors in the field of Information Security research do in fact discuss the limits to what can be determined through the protocol, suggesting a shift in attention from systems themselves to acknowledging and designing for the interactions and understanding this space as primary in terms of how security plays out in practice (Zurko and Simon, 1996; Herley, 2009). Rather than determining things in the protocol, such approaches allow the design space to include and begin from

other sensibilities and to include those who are using and interacting with the system. Questions of the limits to the design space in terms of what a protocol can determine have also entered blockchain debates, primarily in questions regarding 'off or on-chain governance' whereby dynamics outside and beyond the protocol are drawn in as relevant and important. Such a change in perspectives on what matters (from the system architecture to interactions with it) are welcome; however, the articulation of sensibilities other than those of the system itself still leaves the question of that which might never make itself visible, and as such will not demand or set limits on a protocological determination. The ethical and political response suggested by Yusoff in questions of biodiversity is for a kind of 'spaciousness' that allows for the undetermined, the insensible (Yusoff, 2013a, p. 223). This entails holding back on determining things or relations through any one sensibility, not only when and through contestation where something makes itself sensed as mattering, but because, to a large extent, what matters can never be finally or fully known.

Emergence

The insensible does not only pertain to what lays beyond the reach of an algorithmic interpreter, but also internally, raised by the literature as the question of the limits of fully knowing algorithms. The question of what can be known, and whether knowledge, sensibility and relatability are necessary conditions for an ethically and politically informed response, is also debated in relation to the internal dynamics of algorithmic systems. These challenges have been articulated partially with regards to access (proprietary algorithms), and partially with regards to technical knowhow, both in a sense suggesting the need to open the 'black box' and reveal the internal workings such that they can be placed under political (democratic) and ethical scrutiny (Pasquale, 2010; Dodge and Kitchin, 2011; Kitchin, 2014; Seaver, 2014). Blockchain systems, however, are open source by the necessity of their security model and decentralised execution. The fact of their open source nature of course does not address issues of unequal distribution of technical knowledge and code literacy, but even in this realm a lot of work goes into making the coding languages easy to access. In addition, many explanations of different aspects of the systems are given precisely because such explanations are necessary to convince people of the efficacy of the systems and to recruit more computational power and peers to the networks. But there is another aspect to the unknowability of even open source algorithmic systems; Burell describes this as a 'form of opacity centring on the mismatch between mathematical procedures of machine learning algorithms and human styles of semantic interpretation' (Burrell, 2015, p. 3) in her study of machine learning. When unpacking the black box one might simply encounter a form of reasoning that is not within the realm of human sensibility and comprehension.

For Seaver, there is a further issue, namely that a concern with the legibility of technical black boxes gives the impression that 'If only we had access and if only we had the expertise, then all would be clear and we could get on with our critical assessments. I want to suggest that in fixating on access and expertise, we reify a deficient understanding of how algorithms exist and work 'in the wild,' (Seaver, 2014, p. 3). The strategy here then is to trace the effects as they play out, and in a sense, for which complete knowledge and oversight of the inner workings are not always necessary. Amoore, in her work on the emerging dynamics of algorithmic systems, challenges even this strategy because of the ways in which algorithms might continuously change and adapt to circumstance (Amoore, 2016). The implications of algorithmic systems are largely dynamic, emergent and contingent, and are therefore not necessarily known, even to those who develop them (Seaver, 2014). These implications indeed have emergent dynamics, which challenges the idea of being able to fully understand political implications by understanding the intent of designers and engineers. The meaning of one algorithmic design cannot be determined without tracing how it plays out in relation to data and the networks it operates in and in relation to. Big data and algorithms form part of a set of complex, emergent geo-political security practices in which threats and targets are not predefined by any single actor (Kitchin, 2014; Amoore and Raley, 2017). Interactions between technical, geographical, political and legal systems are brought together and described by Bratton, theorist of planetary computation, as an 'accidental megastructure' (Bratton, 2016). Drawn as a stack diagram, he articulates 'layers' that interact and through which different kinds of sovereignties are articulated and enacted by actors that might be more or less able to mobilise such layers and their interactions for specific agendas and purposes.

The *insensible* haunts the sensible here in terms of the systems themselves and their forms of reasoning, which seem to be beyond complete human comprehension, due to both scale and the particular computational modes of reasoning. Regardless, some form of political and ethical response is demanded in and through the ways in which algorithms determine political, economic and security (Amoore, 2006) conditions. In the face of such complexity, mathematical methods have been developed to attempt to address and understand whether, for example, a given system would meet formal specifications (the promise of 'formal verification'). The ways in which such methods relate to questions of social justice, political contestation or otherwise is a broad area of research and action and is still very much in formation.

Blockchain promises more control, in the sense of determining and executing set conditions, but also aims to be out of control, in the sense of being beyond the influence of humans in order to satisfy the claims of neutral algorithmic interpreter. The 'algorithmic interpreter' becoming part of larger computational systems and shifting datascapes in many ways presents its own internal 'insensible', a non-human reasoning and enactment. For some, this

translates into a mode of power and a form of decentralised authority that takes on a non-human life of its own (and to the extent that negative effects of such systems are justified by the system existing and evolving along a logic that is more rational than the human and therefore 'superior' in evolutionary terms in what I have discussed as a 'systems primacy' (Nakamoto, Bridle and Brekke, 2019, pp. 21-22)). In order to make sense of non-human and insensible matterings, I draw on new materialism debates. In the following I discuss three different ways that such debates help navigate the terrains of ethics and politics that acknowledge the non-human reasoning and emergent characteristics of such systems. Most importantly, to be able to do so neither necessitates restoring full control, responsibility and authority to humans, but neither do they necessitate relinquishing all determining agency to an algorithmic interpreter.

2.2.2 New materialisms

New materialisms literature discusses the material world as having its own forms of agency. Instead of mute or dead matter to be manipulated and used by humans, the material world is analysed as affecting humans in ways that challenges assumptions about human control, agency and responsibility (cf. Bennett, 2010; DeLanda, 2004; Haraway, 1991; Latour, 1992). Going further than acknowledging the ways in which materials, landscapes, infrastructures and technology shapes and affects what people can or want to do, this literature acknowledges the cultural practices and experiences that describe a 'vibrant' effects of material things we surround ourselves with and relate to; things as animated, having agency and being alive. Assigning agency to the non-human resonates with and is pertinent to blockchain discussions in terms of how non-human agency is deliberately constructed and implicated into political, economic and legal determination. I argue that this plays out in several ways; firstly as a form of algorithmic animism, where the system is understood as becoming sentient; secondly as techno-scientific collaborations with non-human forces; and thirdly to questions of affinities and alliances that cross assumed divisions between human and machine, or human and biological.

Addressing the question of complex systems as having non-human agency raises some important ethical and political issues. The most immediate is that 'complexity' and non-human agency potentially pose problems for assigning responsibility and enforcing accountability. This theoretical approach at times seems to bypass a perhaps more straightforward tracing of decision-making and power dynamics. In large decentralised systems, control is felt as being elsewhere, but that might simply mean that determining infrastructures have been heavily privatised by entities taking advantage of systemic complexities and obscurities (Greenfield, 2017). And so a new materialisms approach needs to be traced through with care and attention to avoid conjuring a diffuse algorithmic spirit that obscures issues of economic or

political justice. Such issues open up questions of the very possibility of ethics and accountability in relation to non-human systems and modes of decision-making and execution; this is a broad area of debate across AI, new military strategies, finance and so on (cf. Johnson & Noorman, 2014; Noorman, 2014). The aim of involving new materialism debates here however is less to resolve ethical questions in relation to complex systems, and more to be able to describe and explain the different ways in which the non-human is articulated in and through blockchain. It also allows us to address the political implications of these.

Algorithmic animism

Blockchain, as a proposition to resolve problems of authority and power through a decentralised system, is discussed not only in terms of decentralising power across new constituencies but more so as entailing a shift in agency and control from humans more generally to the mediating system itself. Anticipating combinations of blockchain and artificial intelligence (AI), agency and control is sought removed from humans/human-centred institutions. Instead it is assigned to systems with forms of reasoning that are non-human, whereby Smart Contract, transactions, agreements and various other actions and reasoning can take place between digital entities, or physical things (IoT) that have been granted digital identities. In terms of the underlying protocols, these have been noted as an 'internet *techno-leviathan*, a deified crypto-sovereign whose rules we can contract to' (Scott, 2014); as an *algorithmic sovereignty* (Roio, 2018) that might or might not turn out to be benevolent; or as the more metaphysical 'Singularity' and so on. When agency is assigned to and understood as belonging to different kinds of entities with inherent characteristics, these are set up for a relation of comparison and competition about who, human or machine, might be most fit for determining, classifying, ruling and executing a given task.

One way to escape the bind of humans versus an algorithmic authority (either benevolent or malicious), yet not have to conversely assume humans are or should always be in control, is to draw on those approaches to non-humans that avoid assigning definite agency and aliveness to one form over another. One such field is the study of animism. In studies of animism, practices and cultures are discussed in which agency, aliveness and consciousness are not assigned in hierarchical and definite categories – such that humans are the most alive, with the most agency, leaving animals second and rocks and minerals after. Such an approach can be helpful by foregrounding relational understandings of agency and aliveness. This allows for a different kind of openness to the possibility of some algorithmic forms of agency that might indeed come alive and matter to some people and in certain circumstances. But at the same time it is helpful for negating any universal necessity or inevitability of such agencies as mattering or having to matter to everyone. Rather, it is one

form of agency amongst others – whereby the question might become what kinds of relationships are presumed exactly, with who and so on. There are tendencies in blockchain that speculate on and build towards the idea of the Singularity, the idea that artificial intelligence will reach a tipping point at which point an explosion of artificial consciousness will happen that supersede human comprehension and control. In a sense, addressing the field from the perspective of animism is to suggest a shift in the monotheistic underpinnings of notions of 'singularity' and thereby also diffuse the expansionist dynamics implied.

In a post-colonial re-reading of spiritual practices that were in colonial anthropology given the name 'animist', such practices were understood within their own framework of understanding and meaning (Bird-David, 1999; Harvey, 2005). To explain one such example that highlights a relational approach to agency that does not require categories of alive or not: the anthropologist Bird-David describes how the Nayaka hunter-gatherers understand a particular rock to have a spirit. She notes and emphasises that this does not mean that they understand all rocks to have spirits. Instead it is a very particular rock, which fell and hit someone from the community at some point in the past. What she takes from this is that a relation was formed at that moment; the rock came to matter, so to speak. Things become alive when they make themselves felt and when a relationship is formed. The relationship is not necessarily sentimental, but, like most relationships, can be malicious, annoying, entertaining, loving or abusive. The subsequent rituals take care of, develop and resolve such relationships. This aliveness of things, then, is a contingent and context-specific form of mattering rather than a project for a universal registry, list or legal framework around what matters, and also does not necessitate agency, aliveness and mattering as liberal personhood (cf. Appadurai, 2015; Haraway, 1991). This subtle difference, between agency as a force rather than an inherent quality, and aliveness as relational rather than absolute, has implications for how the agencies of things are then translated into political and ethical approaches. In the case of a generalised registry of agency, where agency is understood as 'belonging' to and inhabiting an increasing number of beings, the question then becomes where to draw the line; whether more and more things are recognised as beings and assigned agency. Even more tricky is the question of how such beings are able to 'speak' in and through existing rights frameworks for those of us considered 'alive' (in say a parliament of things, or being a party in say a Smart Contract) (Latour, 1992; Galloway, 2005; Yusoff, 2013a).[14]

Conversely, the exclusions are also context-specific, meaning that things considered to be inconsequential or not living to a given sensibility are not precluded from being alive in terms of a different (human or non-human) sensibility. What this suggests is the need for spaciousness (Yusoff, 2013a) for such other insensible sensibilities to exist and a trust in their

[14] See the Terra0 project for example: https://terra0.org/

claims. More importantly it does not allow for a 'neutral' position because all positions and sensibilities imply exclusion – and so the ethics and politics are shifted towards deliberately enacting such exclusions based on the knowledge and experience at hand and what matters there. In terms of blockchain, this means that it is possible to acknowledge non-human modes of determination and execution while also enacting limitations on such agencies through deliberate and responsible exclusions of these, making decisions about where such agencies should matter or not.

Non-human determinacy

In terms of the techno-scientific, Barad's approach to the scientific apparatus also comes in hugely helpful for opening up some careful pathways through questions of non-human agencies. In her onto-epistemology, it is the particular ways in which all elements come together, the material but also the human and conceptual that determine the potential; what will or will not work in a given design. This includes material elements as well as conceptual such that the possibility of Bitcoin is made up of mathematical models, the idea of a rational economic agent, an understanding that 'centralisation is bad' and the abstract concept of the 'rational economic agent' all come together with the SHA256 hashing algorithm, and the excitement of someone running a full node and the precious metals and fibre optics. There are aspects of a technology that are not fully determined by an engineer or policy maker but by, for instance, some dynamics of mathematics or the capacity of fibre optics. These need to be effectively collaborated with in order for a system to 'function' as intended. Conditions can be made determinate within and for a given system through effectively 'assembling' those (humans and non-humans) present to enact different forms of agency (Latour, 1992) to perform predictable outcomes. Such forms of constructed and predictable determinacy lend themselves to fantasies of control by constructing ever more determinate conditions and apparatuses.

Determinate apparatuses can never sense everything that potentially matters, and this has been discussed above. But Barad's notion of indeterminacy raises a second issue: determinate conditions also open up new fields of potential, new indeterminate conditions. The indeterminate follows continuously behind attempts at determinacy, and so striving for control through determinate systems will never be complete or final, but will only ever continue to open up new fields of indeterminate potential. These may be more or less acknowledged and make themselves more or less sensed in ways that suggest different kinds of response. Processes of determination do not only happen through techno-scientific apparatuses but through 'agential cuts' that can be enacted by and through other intra-actions. Importantly, indeterminate potentials are not the same as the insensible; the insensible might very well be other modes of determinacy (in the Baradian ontological sense),

and, in turn, the apparatuses constructed through techno-scientific practices might very well open up fields of indeterminate potential that are made determinate through other, non-human, biological apparatuses. Determinate modes can have effects on the insensible, both as potential – the field of indeterminacy in a Baradian sense – and also as the unknown modes of determination and sensibility. How to allow for or ensure 'spaciousness' in terms of diagrams of networks then becomes a question worth exploring. It poses a significant challenge to familiar modes of theorising and operationalising in terms of both engineering and political theory because it is a stance *that does not seek to fix things*, neither in the sense of repair nor in the sense of determining in a final manner.

Non-human alliances

Theorising of material relations in de/anti-colonial literature disrupts assumptions about human and non-human agency, foregrounding how humans have also been considered and treated as resources to be extracted, objects to be used or manipulated (Yusoff, 2013a, 2013b; McKittrick, 2014); 'that there is no accumulation without dispossession in both social or geological worlds' (Yusoff, 2017). Agency, understood through such approaches, is not necessarily or always about expanding a circle of what is considered to be alive with valid and recognised forms of intelligence and associated rights, partially because such agency, when assigned within existing political and legal frameworks, is always of a kind that has been predetermined by such institutional frameworks, demanding particular capacities (a language, a way of being and speaking). In terms of blockchain, this means that blockchain systems, far from being 'neutral', require the development of certain capacities that in turn encourage new forms of subjects with the capacities to act within the given system.

A more important point raised through de/post-colonial theorisation of the material is the way in which these shift the focus from needing to determine what is 'alive', 'has agency' or 'is sentient', to a question of the particular quality of the relations formed – propertied, extractive, collaborative, toxic and so on. If the material becomes alive on the basis of relationships, what becomes important is the particular qualities and nature of these relationships. The attention shifts from locating definite sites or beings of agency and control towards the quality of the forms of relationships that are assembled, which make some things more like inanimate objects and other things more like animate subjects. Drawing on the non-equivalence, relationality and contingencies above, these particular forms of 'aliveness' depend on the sensibilities involved and the ways in which these are then translated into and determine relationships. The understanding of agency here shifts from one that assumes human determination in shaping inanimate or controlling semi-animate matter towards one in which what is animate or not is not presupposed but becomes clear only within a given relationship and assemblage.

To put it differently, it is a perspective that takes into account that both humans as well as non-humans can be, have been and are related to in an extractive manner as resources, but also can be, have been and are related to as persons. Alliances and affinities are not necessarily granted amongst humans, who equally are related to as mute matter, objects, resources to be extracted and so on. Instead, this perspective articulates the existence of other forms of alliances that cut across distinctions between, for example, humans and nature (in environmental debates, cf. Yusoff, 2013b) or humans and machines (in post humanism debates, cf. Braidotti, 2013; Haraway, 1991, 2016; Hayles, 1999). Some humans might associate with and defend an animal species or a given natural habitat against other humans, and indeed the affiliation of people with machines and systems that they have created and nurtured (captured and reflected on nicely in stories by Silicon Valley software engineer Ullman, 2013). This also opens up the possibility of an analysis of protocols that focuses on the kinds of relationships that are articulated through and in relation to these.

2.3 The sensible

In this section I discuss the political in the sense of political theorist Rancière's disruption of a 'distribution of the sensible' (Rancière, 2010, p. 92). From the discussion of the *insensible* as a precondition for and challenge to the political, I propose this particular articulation of the political as involving sensibilities as an extension of Barad's onto-epistemological description of how things come to matter. Here I will be tying Barad's agential realism to a more explicitly political conceptualisation of disruption and order, which offers up particular kinds of questions and ways of tracing through what matters politically in blockchain. After discussing the thinking of Rancière in relation to Barad, I draw on the notion of 'diverse economies', articulated by the economic geographers Gibson-Graham (2008). Where Rancière's thinking suggests an understanding of disruption that forces the redistribution of a given sensibility such that new things come to matter, Gibson-Graham's emphasis on already existing diversity suggests an acknowledgement of multiple sensibilities instead, highlighting their changing relationships rather than eventual inclusion. A 'diverse economies' approach thereby points towards the importance of analyses of ongoing and existing relationships between diverse (economic) orders of the sensible rather than assuming, analysing and critiquing a singular (capitalist) reality. Attentiveness to already existing economic diversity external to capitalism in the meantime also opens up questions of already existing diversity internally in blockchain development that does not overlap neatly with notions of capitalism/anti-capitalism, and allows for an articulation of these as mattering politically. I end the section with a discussion of the limits of notions of the sensible in relation to the insensible above, in networked systems and their interactions with the world that cannot be fully sensed or known as such (Amoore, 2016; Ito, 2017).

2.3.1 Disruption and redistribution

The sensible in Rancière's notion of the redistribution of the sensible should be read both in terms of what literally can be sensed (that is seen and is visible and so on) as well as what is sensible, in terms of making sense, being valid and legitimate in a given context (Rancière, 2010, pp. 27–44). It describes a 'common sense' in a given community; that which is considered legitimate speech, action and subject for a given place and time. A distribution of the sensible suggests a spatial and experiential sensibility, and refers to the more explicit formalisation of such order through law and policy, but also to norms, culture, manners of speech and architecture; that which is the result of and continues to enforce a given order of things (ibid.). *The political* is then articulated as anything that disrupts this given order and redistributes the sensible. This can for example refer to struggles around recognition of a new kind of subject(ivity) and rights, or around the ability to perform certain activities and actions in a given place and so on (ibid.) and is therefore a conception of the political that reaches beyond existing political institutions into potentially any context and space. As a diffraction of Barad's agential realist cut (Barad, 2007, pp. 132–185), Rancière's understanding of *the political* can be understood as the disruption, disputes and struggles around what matters and is made to matter (made sensible) that was not previously *sensed* as mattering in the register of a given order. This conception of the political is not limited to institutional, nor indeed human, contexts but can be articulated as anything that makes itself sensible and matter where before it did not. The sensing and mattering of CO_2 in climate debates would be an obvious example, and in the context of blockchain this might be, for instance, cryptographic 'Schnorr signatures'. With this combination of Barad and Rancière, I am making some assumptions of compatibility – the most important of which is the relationship between Rancière's notion of sensibilities (Rancière, 2006, 2010; Dikeç, 2012) and Barad's discussion of sensing and measuring apparatuses as part of onto-epistemological entanglements that have determinate, and material, effects (Barad, 2007). In this sense, I draw Rancière's notion of the political into Barad's quantum physics, relating it to questions of material determinacy and the non-human in an admittedly experimental manner that suggests (and requires) further research and debate.

The concept of 'the sensible' in Rancière's work (Rancière, 2006), having emerged from political contestation of European liberal institutional frameworks, tends to question the way subjects are recognised as having different rights of speech and action within a given political community. Such an order, as a distribution of the sensible, assumes a moment of disruption and then an expansion and new inclusions into the sensible register. This inclusion requires visibility and recognition from a sovereign or a public that is made to sense a disruption, and assumed to eventually acknowledge and include the matter in a redistribution of sensibilities. It assumes a sensing agency (indeed, the *apparatus* in Baradian terms) and in the liberal

context a distributor of rights, whether the state, a sovereign, the public, community or otherwise, that would eventually recognise and include the new subject and arrangement into a new distribution of the sensible. In blockchain, this singular sensing agency, a 'central authority' is in many ways is exactly what is being contested through the proposition of network decentralisation and the involvement of non-human determination. As outlined in the introduction, the proposition and claim of blockchain is to shift the sensing agency from humans, replacing it with what some articulate as an 'algorithmic sovereign' (Scott, 2014; Roio, 2018). In other words, it is not a disruptive project that seeks inclusion into a given sensibility, but rather a project addressing and looking to disrupt the very mode and method of sensing and determining what matters.

External disruption

> Politics revolves around what is seen and what can be said about it, around who has the ability to see and the talent to speak, around the properties of spaces and the possibilities of time.
>
> – Rancière, 2006, p. 12

The notion of the political as a redistribution of the sensible offers a precise yet broadly applicable definition of the concept of disruption as that which forces a redistribution of a given distribution of the sensible. Understanding *the political* as a moment of disruption to a given order points immediately to one of the main claims of Bitcoin and blockchain: that it is a disruptive technology that redistributes who or what validates transactions/information/agreements, determines their value and organises global value flows and the enforcement of agreements. This disruptive promise of both Bitcoin and blockchain is broadly proclaimed to be a redistribution of such capacities and tasks from the given order of things of banks, governments and legal systems to new agencies, both human and non-human. As highlighted in the quote above, this entails not only shifting capacities from one set of agencies to another, but also a translation of such capacities into other forms and spaces. In this case, one might say from politics articulated and debated through policy, to politics articulated and debated through code, mathematics and algorithms. The translation then demands a different set of talents and abilities to navigate these new sites of the political.

Bitcoin and blockchain are frequently claimed as a radical disruption of the established monetary, financial, political and legal order of things (cf. Vigna & Casey, 2018). In the meantime, the financial industry and government departments have begun to take an active role in the field, from hiring developers to funding research and projects, publishing, developing products and so on. And so the question of disruption as a redistribution of the sensible and shift in the given order has begun to be scrutinised within and from outside of

the field in attempts to draw out the exact ways in which the technology is supposed to be disruptive. Legal scholar Herian argues, in a paper that examines the shifting notion of disruption, that disruption has been subsumed within the existing order as simply a competitive new product on the market: 'The blockchain horizon is one in which more capitalism and with it the further and deeper entrenchment of capitalist class power are likely outcomes based on the present course of blockchain research, development and implementations' (Herian, 2016). Rather than redistributing the sensible and making new things *matter*, blockchain applications are pitched as superior services or as opening new markets, but always within the same familiar dynamics of late capitalist modes of economic accumulation. And yet, looking at debates about the latest evolutions of capitalism in the literature – what has been called platform or surveillance capitalism and digital monopolies – these are exactly the industries and infrastructures that blockchain projects claim to disrupt. Herian locates the particular evidence of capitalist co-optation not only in the involvement of existing financial and corporate actors but also and in particular through the question of permissioned or unpermissioned blockchains. This 'particular' offers a far more important insight into the political differentiation emerging in and through the field than a critique based on markets and capitalism, because it stays with the vocabulary and emergent political sensibilities of blockchain and the communities forming around them.

The more explicit and radical forms of disruption proclaimed for blockchain attempts to resist a given distribution of the sensible, understood here as 'centralised' registers of sensibility, including legislation, political acceptance and so on. Rather than disruption followed by inclusion, the ambition is to replace such registers with a different – algorithmic – kind by 'literally coding the world they wish to see' (Manski & Manski, 2018, p. 152), entailing a disruption followed by an 'exit to the internet' (Scott, 2014). The concerns and vocabulary do not neatly overlap with concerns that have formed with and through existing distributions of the sensible then, such as 'anti-' or 'pro-' capitalism or even left and right, but along a technical vocabulary that has gained political significance and draws the political along different lines – such as the line between 'permissioned' or 'unpermissioned'. And so in the construction of new 'digital territories' and 'algorithmic sovereignties', aspects of state functions (security and enforcement of property, for example; see Käll, 2018) as well as capitalist and financial dynamics (markets and profit concerns) are indeed uncritically operationalised and deployed. However, they are done so in new ways and along a different set of ethical and political concerns that are not entirely covered by existing critiques of state, capitalism and financialisation and so are worth tracing and articulating in some detail. Critiques of blockchain concerned with the ways in which they further capitalist tendencies require some careful unpacking in order to understand exactly which tendencies are promoted and how these dynamics are transformed in the process.

Internal sensibility

Understanding the political as a redistribution of the sensible suggests a distribution of the sensible for *any* given setting or context, including the proposition for a technological resolution to political problems. This also entails an internal ordering of what are considered sensible and legitimate subjects, speech and action for different places and times within blockchain assemblages themselves. Meeting the blockchain halfway then, and taking seriously the proposition and possibility of new algorithmic sovereignties and territories, the concern becomes tracing what matters politically to such new constituencies forming around and in these, which should also say something about the order that is proposed and sought to be materialised through blockchain protocols and applications.

My concerns here are the political reasons and reasonings for blockchain, as understood and articulated by the constituencies forming around and through these. Namely, what matters to them, what gave rise to a given assemblage as a political and what holds the assemblage together. I also aim to do so in a way that does not immediately associate these with a capitalist agenda, but takes seriously the diversity of projects and actors in blockchain and their collaborations. That is not to dismiss arguments that the technology might simply reproduce, further and innovate on aspects of capitalist dynamics, but rather to draw a slightly different field of possibilities that foreground a different set of concerns than capitalism/ anti-capitalism. If blockchain is analysed only through the lens of how and where it reproduces capitalism, it misses out on a large part of the story, and also misses out on the potential of the 'disruption' it proposes. To put it bluntly, blockchain sensibilities seem less concerned with 'capitalism' (understood simply as another tool in the toolbox) than with notions of 'centralisation', 'trust' and so on. In fact, the main principles, aims and attributes claimed for the systems quickly appear, signifying the political reasons of the blockchain assemblage: decentralisation, and along with it, disintermediation, privacy, transparency, net neutrality, trustlessness and more. In Chapter 5, I trace this sensibility through cultural histories of decentralised to networks, in Cypherpunk, peer-to-peer communities and open source culture more generally. The intention here is not to claim these as being the 'true' politics of blockchain, but instead to open up two interrelated research possibilities: firstly, to trace emerging distribution of the sensible in blockchain as described by constituencies, descriptions and concepts that are important for shaping the purpose and direction of projects, informing priorities as well as limits to what is acceptable and so on; and secondly to address the concepts and principles that form a blockchain sensibility as mobilising in and of themselves, bringing together people and efforts from across the political spectrum. In some ways, the concepts function as what linguist McGee calls 'ideographs':

> An ideograph is an ordinary language term found in political discourse. It is a high-order abstraction representing collective commitment to a particular but equivocal and ill-defined

> normative goal. It warrants the use of power, excuses behaviour and belief, which might otherwise be perceived as eccentric or antisocial, and guides behaviour and belief into channels easily recognised by a community as acceptable and laudable.
>
> – McGee, 1980, p. 15

The intention is not a linguistic or discourse analysis of blockchain assemblages, although that effort is worthwhile, and has been commenced by, amongst others, Reijers & Coeckelbergh, 2016. Instead, the question is the specificity of these concepts and the way they came to matter politically in these blockchain assemblages. The anthropological work of Coleman (Coleman, 2009, 2014) amongst hackers involved in the field of InfoSec (information security) and the amorphous hacker network Anonymous is a valuable resource here as it highlights the particularities of the culture, ethic and politics of different internet cultures as important in shaping targets and strategies, and in defining the specific logic of who is considered an ally and who is an enemy. This cultural history and detail has largely remained untold, both in the literature around blockchain and across blockchain assemblages. This context is taken for granted, in part because the concepts describing what matters in the technology are indeed 'equivocal and ill-defined' (McGee, 1980, p. 15) in the political and social meanings, if not also in the technical. Such vagueness, however, in some sense holds the assemblages together regardless of differences in terms of how they are implemented and understood. It also allows for alliances between what might otherwise seem contradictory socio-political positions. More importantly, however, the differences between their interpretations became the very space in which a new politics is negotiated and formed in and through disputes around the definitions, operationalisation and materialisation of blockchain epistemologies.

The explicit articulation of these 'ideographs', principles and politics and the excavation of their histories in internet-based political culture therefore contribute to opening up space for political potentiality beyond proclamations about capitalism. I take seriously what matters to those developing the technology as an integral part of shaping the field of political possibility along and through a different set of concerns. This entails tracing the vocabulary, principles and intentions of peer-to-peer, Cypherpunk and open source internet cultures to understand the particular form of disruption proposed through these sensibilities – and to do so in order to carve out some lost spaces of political possibilities in the field. By placing Bitcoin and the blockchain into a longer history of decentralised systems that stretches back to the '90s (Troncoso *et al.*, 2017), the fidelity more broadly is to these principles and to computation, into which economic theories are operationalised in different ways. The attraction of Bitcoin, for many involved in the development and maintenance of peer-to-peer decentralised networks, was the possibility of developing a decentralised system that would 'pay for itself'. It pointed

towards the possibility of economic autonomy for such systems and the communities that run them. This does not mean there is an entirely uncritical approach to modes of accumulation, but rather that these do not overlap in any neat way with what might be recognised as right or left political economic thinking or solely concerns about capitalism. Instead, a different set of concerns is foregrounded, brought together through broad concepts of decentralisation, consensus, trust and so on, whose ambiguity both mobilises across the political spectrum as well as articulates potential contradictions with late capitalist modes of accumulation as areas of legitimate political dispute – even when they take the form of new business models rather than new political parties or social movements. The 'blockchain' that suggests itself for political analysis through this onto-epistemological cut of the *sensible* includes descriptions and concepts by the constituencies formed around blockchain as a project, their definitions and articulations of the political and reasons for being involved, both as a disruption externally and a proposition for a different sensibility and sensing agency.

2.3.2 Diverse economies

Diverse economies was proposed by Gibson-Graham as a subject field and emerging research community in a paper seeking to intervene into critical economic geography by foregrounding already existing diversity of economic practices (Gibson-Graham, 2008). The intervention sought to challenge the assumption of capitalism as an all-encompassing system, and problematise the ways in which alternatives are thereby marginalised, overlooked and under acknowledged. For some time now, they argue, critical literature on capitalism has simply not been helpful for expanding other economic modes and possibilities. They argue that 'other worlds' than a capitalist one already exist but are underappreciated – also, and importantly, by critical thinking concerned only with the new frontier of capitalist accumulation. Instead, they suggest, non-capitalist economic activities, when considered together, in fact outweigh strictly capitalist ones (Gibson-Graham, 1996). Capitalism can therefore realistically be considered as already only one among many economic modes, and as indeed dependent on such other modes of re/production. By foregrounding already existing alternative economic practices, these can in turn be validated, recognised and strengthened.

An important possible oversight in analyses that seek to conceptualise a given order of things and the potential for its disruption is that a given distribution of the sensible is never singular. There are always multiple distributions and sensibilities that coexist and continue to do so that are often excluded in order to maintain coherence. A diverse economies approach to the political economic sensibilities of 'blockchain' helps to articulate diversities and potentials amongst blockchain projects and in relation to existing capitalist dynamics and assess these less as either full blown hyper-capitalism or an alternative that either fails to, or succeeds in,

replacing existing capitalist and financial systems, and more as propositions and potentials within a diverse field of economic dynamics. A diverse economies approach also radically shifts the focus of attention from building internally coherent systems to an understanding and treatment of the interrelationship with other existing systems as mattering at least as much. This poses a challenge and promotes an interesting area of political and strategic research in terms of blockchain protocols and their design, such that interrelationships and dependencies on for example exchange rates and the dollar or yen is brought into the narrative of how such infrastructures operate politically, rather than dismissed as irrelevant or unfortunate speculative behaviour. The approach, in other words, opens up a significant shift in the treatment of blockchain (and capitalism) as self-coherent systems, both internally and externally.

Diversities instead of 'externalities'

Gibson-Graham's diverse economies approach can be read as a contribution to a longer history of feminist political economy. A major contribution of the field has been to situate capitalist modes of production in relation to, and as dependent on, reproductive work 'outside the factory'. The aim was to make work done by women and others in the home and communities visible and recognised as mattering and having value in terms of the economy. The important contribution of Gibson-Graham is that rather than conceptualising other modes of re/production as 'externalities' to be included into and accounted for in a general economic sensibility, they argue for acknowledging diverse economic spaces in their own right. This repositions such activities from external and marginal with demands for inclusion, to one of diversity, instead considering the relationships and interfaces between them and a capitalist system, or other interfacing economic systems, as ongoing sites of political articulation.

The main lesson here, both in terms of capitalism and blockchain systems, is that it is a fallacy to treat such systems as singular and hermetic as they are always in relation to other systems and spaces, the relations, boundaries and interfaces of which are constantly being negotiated. In other words, different economic modes and ways of being should not be treated as 'external', but rather understood as differentiated – an ongoing continuous difference, the relations between which can be configured as extractive, collaborative or otherwise, but which are there regardless. This challenges teleological tendencies in literature on blockchain (and capitalism), where the imaginary is singular, necessitating eventual overthrow of existing systems and takeover by new and better ones. Instead, a diverse economies approach acknowledges that there are already, and always will be, other economic modes, and these need to be acknowledged and treated with careful attention. A diverse economies approach suggests a different possibility of political analysis and strategy, namely a deliberate consideration, articulation, design and shaping of coexistent and

interdependent economic modes. The project then becomes less about the disruption of a singular sensibility (whether articulated as 'capitalism' or 'centralised systems') to be followed by a redistribution of the sensible through inclusion of a previously marginalised 'external' into the modes of a reformed system, and more an expansion of diverse economies and reconfiguration and deliberate articulation of the terms of their relations to a capitalist economic sphere.

Internalities

These lessons pertain not only to analyses of a relationship of blockchain projects to capitalism and other already existing economic diversity, but also internally in the blockchain communities in terms of how blockchain protocols tend to be described as hermetic systems by excluding dependencies and relations with existing economic, political, legal, infrastructural (and so on) systems. Computational or protocological affiliation in this sense serves the role of 'capitalism' in Gibson-Graham's analysis (Gibson-Graham, 2008): a totalising explanatory framework, that is either foregrounded in utopian and dystopian narratives or sits in the background as an omniscient 'neutral' substrate for the coordination of decentralised behaviour (cf. Buterin, Hitzig and Weyl, 2018). In adjusting the insights of diverse economies towards the exclusions that are performed in order to articulate blockchain coherence, I aim to direct attention to the ways in which, for example, 'cryptoeconomic' dynamics necessarily relate to, and will continue to relate to other economic spaces. This shift in perspective brings out questions that are often sidelined in discussions in the blockchain community as unfortunate dynamics that are not relevant to the underlying technology, while being hugely important practical issues. These questions relate to things like regulation, exchange rates and geo-political, environmental and geological differences; the many ways that cryptocurrency and blockchain projects relate, resists, incorporates or competes with existing economic systems and processes. These matter for how the political effects play out and should therefore be taken seriously. In fact, interrelation with other systems is an extremely strategic point for articulating power dynamics in terms of flows of resources, touching on questions of sovereignty, autonomy and control.

There are three things to take away here. In Baradian terms, the 'cut' of what is considered relevant or not in a description of blockchain matters, and a diverse economies approach is a cut that brings to the foreground 'the political' in articulating relationships between already existing as well as potential diversity of systems and sensibilities. What is considered important politically, then, is the articulation of relationships with a diverse set of economic spaces and modes rather than a singular analysis of decentralisation in relation to centralisation (or capitalism). The configuration and shaping of those relationships matter; it can be one of invisibility and 'externality', it can be one of exchange and so on, but what is

important to keep an eye on is the power dynamics that are articulated through these relations and how different spaces are expanded or suppressed in the process. Recognising and foregrounding relations does not in and of itself address the politics and power dynamics of such relations. It merely recognises these as a site for (potentially violent) political negotiation and articulation. Secondly, this lesson on already existing diversity pertains not only to critics but also to proponents and developers of blockchain. What is or is not considered relevant to blockchain protocols matters. Where the line is drawn around the design space of what the protocol should determine matters, but more importantly, the way that line interfaces and relates to other systems is not a marginal question that can be left to happenstance but is hugely significant in determining the effects of a given system. Finally, and importantly, by focusing less on some complete story of what blockchain *is* and more on how it becomes in relation to different economies and contexts, we begin to see what matters to the community and the field of possibilities and tensions in terms of its development paths.

By drawing in Gibson-Graham's notion of diverse economies, my aim is to open up a space for research within critical blockchain literature that does not take its likeness to capitalist economic modes as its necessary starting point, but to instead look towards the diversity of economic spaces and the articulation between them as important points of political possibility and determination. The blockchain assemblage itself is not fully determined through capitalist economic ideas, but has a slightly different notion of 'disruption' and set of concerns related more to computation, decentralised networks, information security practices and notions of 'authority', which in fact open up a different field of potentialities in terms of how the technology could play out. I argue that it is important to take the concerns of the communities building the protocols and platforms seriously as a factor in the shaping of the political possibilities in the space. These open up further questions to be explored in and through research into emerging blockchain constituencies, including identifying the ways that blockchain is described as relating to other economies, systems and spaces, how these relations are understood politically and how they play out. This work seeks to carefully draw out potential contradictions and fault lines between existing sensibilities and those that blockchain open up for, to understand the specific kinds of disruption proposed and made to matter.

2.4 The dissensible

In my third and final Baradian 'cut' I articulate the *dissensible* as an approach to the political that addresses the persistent emergence of incompatible positions and the ways in which these are expressed and negotiated. By using the term 'dissensible' I draw on political theorists Laclau and Mouffe and their emphasis on 'failed unicity' (Laclau & Mouffe, 2001;

Mouffe, 2012, p. 29), as well as Rancière's work on dissensus as the basis of the political (Rancière, 2010) and the precondition for a 'redistribution of the sensible'. The proposition of Bitcoin and blockchain was, and still is to a large degree, to translate political and economic questions into a technical problem of decentralised consensus, and then solving it through technical means. The debates in the previous two sections address firstly the matter and material politics of blockchain and the *insensible* as the limits to what can be political known, and secondly how blockchain came about as a political sensibility. The dissensible is a response to the idea of a 'consensus protocol' as resolving the problem of the political, in any final manner, drawing out and highlighting what might be the *dissensus protocols* in operation, protocols understood here in a broader sense of the formal or informal ways that disagreement and incompatibility is dealt with. The dissensible addresses how disagreement and incompatibility is managed within the proposition of a technical solution to the political and the governance methods developed and employed to do so. The 'blockchain' that suggests itself for political analysis through this third set of debates includes core developers, full nodes, miners, developers mailing list discussions, GitHub processes (forking, pull requests and so on), in fact all the actors that are involved in contesting or maintaining a given version of the blockchain. In this final section, then, I discuss the thinking of political theorists that take as a starting point a constant potential for dissensus, and therefore the need for the political as a realm in which to resolve such dissensus under conditions of incompatibility.

2.4.1 Dissensus protocol

Mouffe and her collaborator Laclau, ground their understanding of the political in a conceptualisation of the universe as fundamentally divided 'where the primary ontological terrain is one of division, of failed unicity.' (Mouffe, 2012, p. 29; Laclau & Mouffe, 2001). They critique perspectives that are based on the notion, metaphysically or otherwise, of a unified whole, because the articulation of such a whole always entails exclusions of that which was not included in the description. This conception of collectives as always and necessarily exclusionary argues for the persistence of the political in that there is always the possibility of excluded positions to make them selves felt, and therefore there is always a need to be able to negotiate these. Mouffe refers to this as agonism (Mouffe, 2005, pp.19-21), which I treat as the possibility of dissensus. This failed unicity, they argue, entails that there will always be a need for some kind of terrain through which to negotiate differences and incompatibility as and when it arises – the political, in other words, will never be solved and is a constant condition. There will always be something external to a defined collective, always some form of border determining the edges. In a Baradian sense, what matters are how such exclusions are articulated, and the ways in which they are attended to or managed when and if they make themselves felt. Through this understanding then, the political is never solved; it is

simply reconfigured. And so, in blockchain systems, while the protocol seeks to resolve questions of how to conduct politics, in a sense automating aspects of the conduct of politics, the political is thereby shifted into the realm of the technical, and is played out in technical disputes over protocol changes. A focus on dissensus thereby initially offers a methodological approach as to how to trace the political in and through blockchain systems, by paying attention to conflict, technical or otherwise, understanding these as political and analysing the ways they are resolved. Looking at development processes and pathways and code governance also reveals how things might have been and still could be different.

Mouffe discusses the issues of dissensus in relation to exactly such institutional forms that were supposed to accommodate for processes of mediating dispute through political debate and deliberation, namely European/US liberal democracy in the years preceding the 2008 global financial crisis (Mouffe, 2005, pp.83-89). She looks at what happens to the possibility of dissent in contexts where an overall consensus about the *means though which to address dissensus* is assumed. The reason for this is precisely because while this political climate prided itself on allowing free speech and open debate, the institutions and political framework itself were in the process assumed to be universal and unquestionable (ibid.). And so, her argument is that in the specific context of liberal democracy there is a certain space for disagreement, a legitimate kind of dissensus, but only within the predefined forms and formats of established institutions. In her account, the effect of such an inability to politically question the institutions and economic organisation that represented the liberal democratic project was to marginalise dissent (Mouffe, 2005, pp.76-83) . This attention to the political and the ways in which it can or cannot be expressed point towards two further questions of blockchain as a proposition to resolve or automate the political – namely, what are the broader effects of reconfiguring the political as a technical question, and secondly, how is dissent, as an ongoing possibility, managed in these systems?

Mediating the political

In this discussion of the post-political liberal democracies, Mouffe opens up questions around the effects of assuming these as neutral and universal mediators of difference (Mouffe, 2005). She is concerned with the effects of shutting down the possibility of the political understood as agonistic and dissensual. In her analysis of liberal democracy, the liberal consensus by assuming particular forms through which politics would be conducted in turn reconfigured the political (agonistic forms) as moral debate, shifting fundamental differences into a realm of morality (Mouffe, 2005, pp.72-76). Far from solving 'the political', this instead turns what she terms 'agonism', which I address here through Rancière's notion of 'dissensus', into a violent form that in turn is also expressed through post-political absolutes. Mouffe argues that in liberal democracy what was previously the Left and the Right has been reconfigured as moral

questions of 'right and wrong' (Mouffe, 2005, p.5), meaning that this is no longer a dispute between fundamentally different but nevertheless acknowledged positions, but instead one between a perspective that has the right to exist (liberalism) and another which does not (that in turn become 'extremism', 'nihilism' or 'populism' and so on). And, she argues, this reconfiguration creates violent responses from those who hold positions that, from the perspective of liberal democracies, are not supposed to exist (Mouffe, 2005, pp.76-83). Dissensus can be configured as indeed political questions or pushed into other forms such as morality in her example. Such other forms through which to deal with dissensus never finally solve the issue, but do change the ways these erupt and are made to matter, and therefore matter in themselves.

What I suggest here, via Mouffe, is that the form of mediation and resolution of dissensus will affect the ways in which disagreement with the particular form of mediation expresses itself. The medium matters, so to speak, for the ways in which the political is made to matter. And so reconfiguring the political into a technical problem and solution might also reconfigure the way agonism or dissensus can be expressed and made itself felt both in terms of internal dispute over technical changes and also with the protocol as a mediating form in itself. This raises the questions of how dissensus is resolved in blockchain assemblages that claim to have solved dissensus already through algorithmic means, and also what expressions of dissensus is considered legitimate and what which are excluded. If the protocol becomes what the liberal democratic institutions were in Mouffe's analysis – the only legitimate medium through which to conduct politics – then the political, as incompatible difference, as the dissensible, will make itself felt elsewhere in unexpected forms.

The blockchain space saw a significant shift in perspective and attention following some major disputes around code changes in Bitcoin and Ethereum, which made the community start to consider questions of governance and in particular protocol governance and the extent to which it lives up to the ideal of decentralisation. The management of disagreement and incompatibility was put centre stage and new forms of governance began to be articulated with new justifications of these. Forking code repositories, for example, was articulated as the means through which these systems would manage and accommodate dissent in the governance of code (the topic of Chapter 6). But the question of agonism raised by Mouffe is precisely *not* aimed towards seamless management of different perspectives on what matters (which to some extent was the aim of liberal democracies), but rather to allow the possibility for different perspectives to meet and clash on a variety of territories. Just as the political made itself felt in the blockchain world through protocol disagreements, it was immediately and swiftly integrated into questions of governance, meaning the most effective management of differing positions. And so a final resolution of the political problem of difference was once again assumed through ever-more sophisticated mediation mechanisms

combining markets and networks into new configurations. The political, in the meantime, cannot quite be contained within the notion of governance. The concept of governance tends towards management while the point of Mouffe's work is that the political cannot always be managed and will erupt in illegitimate forms.

Neutralising the political

It is only if the political is considered something to be finally resolved that the need for a neutral mediation emerges. A neutral mediator would then resolve issues of difference and agonism as and when it emerges, and, rather than addressing difference, the political is therefore addressed through a search for neutral or universal principles upon and through which such a system can be built. There are, in this sense, significant similarities in the claims made of both decentralised protocols and Mouffe's reading of liberal democracy: that they mediate and provide the substrate for coordination amongst competent free agents, and that they do so in the most rational and just manner. The political aim of decentralisation can arguably be understood in this manner to establish a maximum freedom through a substrate that coordinates behaviour in a supposedly neutral and fair manner. A response then, to both technical and institutional claims of neutrality, has been to re-politicise these and show the ways in which they require certain capacities in order to navigate effectively, with implicit biases and inequalities that follow.

By politicising such propositions for neutral mediation and resolution of difference seems to open up a problem of infinite regression: if the protocol is political, then there should be a means for voicing dissent about the protocol. If the means for voicing dissent about the protocol is also political, then there should be a means for voicing dissent about this too – and so on. This plays out in blockchain through discussions and questions of governance mechanisms, and in the ways in which many projects – particularly after the major politicised protocol disputes – sought to position themselves as ever more universal, neutral technologies, from platforms, to protocols, to language, in order to be that neutral substrate upon which difference can emerge and play itself out. However, if the question is not about resolving the problem of the political in any final manner, the conceptual problem of infinite regression disappears. Instead, attention and consideration can shift towards the ways in which a given reconfiguration of the political – in this case into a set of technical problems and management processes – affects and changes the ways in which dissent and dissensus is expressed and resolved both internally through the protocol and around it through those that chose not to engage via the protocol. Dissensus, and what Mouffe understands as the fundamental condition of agonism, is the continuous possibility of negation of any common substrate in the first place, whether protocological, ideological, religious or institutional. And, to draw Rancière back in (2010), such a negation can be hugely generative in that it

redistributes and redefines the landscape of what matters, what was previously insensible (Yusoff, 2013a) or what in the case of blockchain might be better understood as the redistribution of the sensible and possible, and a literal development of a digital territory and space where new things are possible and new constituencies are formed (Roio, 2013). This also raises the question of what holds the assemblage together and where the limits of acceptable dissensus lie before something is simply considered an invalid position and excluded, and how such forms of dissensus are expressed.

2.5 Conclusion

In this chapter I have drawn together disparate theorists and debates in order to propose three 'cuts' in the political significance of blockchain. The first cut is framed by Barad's treatment of determinacy and indeterminacy as not 'belonging' to a specific field, discipline or form of agency (social, algorithmic or otherwise), but rather as entangled, whereby phenomena are made determinate and made in/to matter by all sorts of sensing agencies drawing 'cuts' and making things (into) matter (Barad, 2017, pp. 132-185). Things are determined in many different ways by many different forms, making the question one of which is the most appropriate and beneficial and for whom, rather than making a necessity of an algorithmic one on the basis of ideas of objectivity. I elaborate this cut further by drawing in Yusoff's discussion of the 'insensible' (2013a): not only are there multiple ways in which an indeterminate field is made determinate, there is also the matter that these ways might not be immediately sensible. Whether algorithmic, animal, mineral or otherwise, these suggest sensibilities that might never make themselves explicitly knowable and sensible to a given registry. This cut further suggests that instead of any singular human/legal/political/economic blockchain registry of what matters, there are affinities and alliances that already cross these categories. I suggest that this enables an approach to further analysis of blockchain protocols whereby their determinate qualities might be interesting and potentially useful, but are not assumed to be the only or most appropriate means for determining things. The *insensible* therefore suggests a detailed analysis of the very particular kind of determinacy enacted in and through blockchains, its limitations and why parts of the blockchain community find it to be a better way of resolving and determining the political. This is the topic and focus of Chapter 4 and the first 'cut' on the political matter of blockchain.

There are other angles and debates that could have been brought to bear on questions of blockchain protocols and their political and ontological implications. One major omission that is worth briefly highlighting here is the literature and debates that articulate network infrastructures as intermediating and making possible a 'collective consciousness' whereby internet infrastructures facilitate forms of collaboration where the whole is greater than the

parts (cf. Bria and Roio, 2014; Kennedy *et al.*, 2001; Halpin and Thompson, 2009; Rifkin, 2014; Rogers *et al.*, 2015). Instead of conceiving protocol and algorithms as new forms of sovereignties beyond human control, such articulations and projects aim towards a different understanding of democracy, whereby network infrastructures make possible new forms of collaboration, knowledge-sharing and decision-making that reorganises what is politically possible in important ways – towards a form of direct democracy at scale. I chose to omit this very important set of debates for two reasons. The first is that the mood and analysis around such debates has shifted significantly with the growing awareness of the ways in which network infrastructures are used for commercial, geo-political and state-based surveillance and targeting. This decision, to address the very preconditions of debate, has also meant that other opportunities in terms of blockchain protocol analysis – for instance in-depth comparative analysis of different consensus protocols in the field – are beyond scope, yet have formed an empirical backdrop nevertheless. Secondly, and related to the first point, this shift in mood and awareness seemed to lend resonance to ideas forming part of a blockchain sensibility that is heavily concerned with not only security and privacy but broader issues also. In other words, I found that limiting the scope to address ideas, attitudes and a sensibility coming out of blockchain proper to be a more pressing and compelling concern. Assessing the possibilities of using blockchain for such purposes of new forms of democratic life or more egalitarian economic dynamics is absolutely related to but beyond the immediate scope of this thesis.

The second 'cut' is framed again by Barad, but this time more explicitly assisted by Rancière's notion of the sensible (Rancière, 2010, pp. 27–44). With this cut, I suggest that there is a sensibility that holds blockchain together as a recognisable assemblage, despite significant differences in terms of political and economic ideas. This sensibility can indeed present a disruption and redistribution of other sensibilities. I draw on Gibson-Graham (2008) to sharpen this cut, such that both 'internal' and 'external' diversity is taken seriously in the analysis. This means that the diversity of economic and political ideas in the blockchain assemblage suggests that what holds the assemblage together is not primarily economic or political ideas such as 'capitalism', but a different sensibility that intersects with capitalist notions or indeed other economic ideas in different ways. It also suggests an external diversity, such that blockchain systems, projects and protocols are never a wholesale replacement of some complete system. This suggests that analyses of projects and protocols cannot be so easily addressed as hermetic complete solutions to the political, but rather should be addressed and analysed in terms of their relationships and dependencies on other already existing economic and political dynamics. Drawing out and understanding such a blockchain sensibility and its provenance is the topic and focus of Chapter 5, and this thesis will discuss the relationships to both an internal and external diversity.

The limitations of this approach are largely due to the priorities being an intervention on the terms of debate. A potential alternative theoretical approach might have been to draw directly on heterodox economic literature, including a broader field of feminist or commons-based economics. This might have more directly achieved what I discuss as a possibility by drawing in Gibson-Graham's notion of diverse economies – namely, to redraw what is possible and what matters in relation to blockchain and cryptoeconomics, and not assume a singular capitalist reality. My admittedly difficult decision to not take this particular theoretical approach was in large part due to my selection of case studies, Bitcoin and Ethereum, on the basis of being the two largest projects that arguably set standards for the rest of the blockchain industry. If I were to say anything about a blockchain political sensibility proper, these cases would need to be a primary focus. An alternative approach might have been to include heterodox economics, and work with comparative cases to flesh out such differences and diversity. This was indeed the initial intention, and, as I explain in the introduction and in Chapter 3, I had included the Faircoin case for this reason.[15] However, by doing so, I would have opened up a different set of debates focusing more on economic theories and their enactment through technological infrastructures. I made the decision to address the political and articulate a blockchain sensibility proper. This does open up interesting possibilities for further theoretical work, however, to understand the relationships between such a sensibility and political economic ideas. Similarly, and on the topic of the economic, another body of literature that I have largely excluded from discussion is that pertaining to monetary theory and complementary currency debates in relation to cryptocurrencies (cf. Bollier, 2014; Peters, Panayi and Chapelle, 2015; Roio and Sachy, 2015; Roio *et al.*, 2015; Scott, 2018). Again, the decision to omit this literature was largely because the focus of this thesis, and this particular analytical 'cut', is blockchain and the political more generally, rather than currency applications and their economic implications, although these do interrelate as I discuss further in Chapter 5.

The final Baradian cut that I have set up in this chapter, once again with Barad and Rancière, but this time sharpened by the political theories of Mouffe, has allowed me to introduce my concept of the *dissensible*. Here, I point to the political as an ongoing potential for things to be different, for incompatible sensibilities to arise. This suggests two issues that I discuss through Mouffe and Barad: firstly, that such incompatibilities raise the question of how they are resolved, not in any final manner, but as delineating the contexts and conditions through which incompatibility is considered to be best negotiated; and secondly, that the method for resolving such incompatibility matters, qualitatively, by assuming and requiring certain capacities over others. This cut suggests that the issue of consensus is not resolved in any final manner by a blockchain consensus algorithm, but merely shifts the question of

[15] See https://fair-coin.org/ see also https://holochain.org/ as another example of heterodox economic thinking in relation to blockchain, or in this case hash trees rather than blockchains.

dissensus to other realms, layers and modes of expression. As is discussed and exemplified in Chapter 6, this requires an analysis of the governance of the protocols themselves and their mode of resolving consensus. Solving the political through a network protocol means that dissensus is translated into a question of security, attack vectors and honest or malicious behaviour.

My discussion of Mouffe, Rancière and Barad as a way to draw this cut once again leaves much literature that could have been theoretically fruitful. And, again, the motivation has been to focus on explaining and shifting the terms of debate by articulating the question of dissensus, and the qualitative importance of how the dissensible is resolved. This has left perhaps more direct approaches to the question of protocol governance beyond the scope of this thesis. Related debates and literature that might inform protocol governance more directly pertain to management and organisational theories, as well as certain branches of political theory that deal with decision-making structures and processes, in particular decentralised ones. A second, slightly tangential but potentially fruitful area would also have been discussions of sovereignty as a way to articulate a more precise remit of protocol governance. Because blockchain in many ways is a technology that explicitly aims to delineate and secure a kind of networked space beyond the control of perhaps more traditional 'sovereigns', there is a project and claim here of articulating new forms of sovereignties. These include projects (see for example Bitnation) and ideas for specifically digital, planetary and 'self-sovereign' kinds (Gupta, 2015; Bratton, 2016; Reijers, O'Brolcháin and Haynes, 2016; Smolenski, 2016).[16] [17] Such debates and cases are unfortunately beyond the immediate scope of this thesis, but suggest some interesting areas for further research.

A limitation, or rather tendency, of a Baradian approach is that by drawing concepts from quantum physics into the political, social and technical, such as 'entanglements', 'determinacy' and 'indeterminacy' and so on, we might obfuscate a more direct description of a social world and political stakes – who is doing what in a given situation. This requires some careful attention, and necessitates extra descriptive work such that Barad's concepts instead can be effective for opening new angles while remaining precise. I turn now to the next chapter in which I discuss the research questions that I have sought to answer through these three cuts, the methods and methodologies and case studies that I have employed to do so.

[16] https://tse.bitnation.co/
[17] See for example https://blockchainhub.net/self-sovereign-identity/ and https://www.brighttalk.com/webcast/16693/329797/blockchain-and-self-sovereignty-in-the-age-of-consent

3 Research methods

The main question that I seek to answer in this PhD thesis is the question of what matters politically in blockchain technologies. By 'matters' I mean literally mattering in the sense of making a material difference for what is developed and how, and how this in turn plays out. What I want to find out are the aspects of the protocols and their designs that are key for determining one outcome over another; in other words, a potential moment and place of decision and difference, which might in turn be a potential site of *the political*, the negotiation of such difference. The reasoning is that if blockchain is a technology aiming to resolve the political – a 'technical system' that 'off-loads authority onto a transparent and public consensus history, created and validated by the protocol and some of its users' (Kreutler, 2018) – then the key for understanding this particular resolution would be in the protocol itself and the ways in which it organises, settles and enforces a 'consensus' in the network. My motivation for, in this sense, insisting on 'the political' in a technology claiming to resolve it is motivated by a concern for the possibility that things might be different, can be coded differently and that there is nothing inevitable nor necessary about a particular consensus protocol design.

Because of such a focus on technical determination and the politics of protocols, my initial assumption was that consensus algorithms implied a shift in site and form of the political decision from what might normally be considered political questions, disputes and disagreements to technical questions about the very means for their resolution. Therefore the moment and site of political decision would also have shifted to the design and coding of the protocols themselves – the decisions made by protocol developers, systems designers and cryptographers – as mattering politically for determining the effects of this technology. This assumption was to cause some analytical difficulties (discussed 3.2.4 below) but, in the meantime, it informed the scope of my methods and the focus of my research setting: the whitepapers themselves, the ideas and assumptions informing their design and the communities developing these were the main focus of and setting for my research, informing the questions I looked to answer and the methods I employed for doing so.

In this chapter, I describe my methodological design and its implementation and also reflect on its limitations. The chapter is structured as follows: in section 3.1 I describe my research design and how my research questions led me to take a case study approach, as well as the particular selection of cases. During the course of my analysis I dropped one of the cases, namely Faircoin, and so I briefly discuss the reasoning for this and the ways in which the case nevertheless has informed aspects of the research. I conclude the description of my research

design by addressing my own positionality in the field and the ethical questions arising from this and from studying the blockchain field more generally. Section 3.2 gives an overview and description of the different phases of my empirical research and the methods I employed in those phases. In 3.3 I describe the approach and process of data analysis and the path I took arriving at the overall structure of this thesis. Research questions will always in themselves entail certain assumptions and I have as much as possible sought to make these explicit and to discuss alternative approaches that might have been fruitful and the reasons for my decisions. I conclude the chapter by reflecting on the main assumptions and limitations of my methodological design.

3.1 Research design and positionality

In this section I describe my research design, the research questions that informed it and discuss its limitations. My research design and methods were heavily driven by my research questions, which took me across mediums, places, disciplines and contexts. The research questions are therefore key to the decisions I made during my empirical research and form the backbone of my methods. As discussed in the introduction chapter, three main questions informed my research design:

1. How do the developers and users of blockchain understand, represent and seek to shape the political implications of the technology in terms of decentralisation, trust and consensus?
2. Which are the active 'mediators' in the blockchain assemblage, what difference do they produce and what political effects do they have?
3. What are the political differences between blockchain-based developments, and where and how are these expressed? (E.g. in the code itself, in the organisational structure of the developer community, amongst the user-base or elsewhere?)

The form of these three research questions suggested that their answers may not necessarily be found in any one particular place, document or interview, but that anything *potentially* mattered a piece of code, the location of a given conference, a discussion board, assembly on the group chat application Telegram, keynote speech or logo of a given project. The research process, then, was more akin to tracing clues. Attempting to answer these three questions required going in-depth into the ideas informing projects and protocols as well as the contexts, disputes and debates surrounding their development. This led to a decision to take a case study approach to focus on a limited research environment rather than address the blockchain field as a whole.

3.1.1 Research design: case studies

I initially chose three case studies – Bitcoin, Ethereum and Faircoin – with the aim of understanding processes of deliberate differentiation and enabling a comparative approach between these. The intention was that each of the cases would reveal different aspects of the ideas and possibilities in blockchain technology, as well as allowing for a comparison that might reveal political intent and effects. The three case studies were therefore selected on the basis of providing a good general understanding of 'blockchain' as well as the particular instantiations of different political assumptions and aims. This justification was later confirmed as the Bitcoin and the Ethereum networks grew to become the largest and second largest blockchain networks, therefore setting much of the standard that the rest of the industry and community would respond to, while the Faircoin project drew from and articulated a distinctly different and politically motivated understanding of decentralisation, trust and consensus. It also became clear that not only were there stated differences that covered unique angles on the technology in each case, but that this was also materialised in different consensus algorithms at the core of each project that pointed to deliberately different development pathways. The first was the initial invention of consensus algorithms in Bitcoin, using what is called 'proof-of-work' cryptographic hashing (explained and discussed in detail in Chapter 4). Ethereum then looked to change the Bitcoin protocol because of issues of energy waste and possible centralising tendencies, developing a 'proof-of-stake' algorithm to take its place. Finally, Faircoin invented a 'proof-of-cooperation' algorithm with the intention of removing market dynamics from the protocol operations and introduce more community-based oversight drawing on socio-political rather than technical understandings of trust and consensus.

Over the course of my analysis, however, I decided to let the Faircoin case recede to the background, as it opened up a range of new debates and themes that were beyond the scope of this thesis. The Bitcoin and Ethereum cases raised the question of the possibility of replacing aspects of political decision-making and enforcement with forms of algorithmic mediation. The consensus algorithms in their architectures became propositions for a resolution of the political in and through an algorithmic or protocological agency, which Roio terms 'algorithmic sovereignty' (Roio, 2018), and which I discuss as a form of animism in 4.2. While the Faircoin case served to highlight this very novelty, to do it justice as a case study in its own right required drawing on and opening up a different set of debates, including but not limited to social movement organising strategies, heterodox economics and alternative and social currency projects, all of which are highly relevant to blockchain discussions and developments but require and deserve a fuller treatment in their own right. The focus, in other words, became what might be articulated as common *sensibility* amongst blockchain projects, such that it is possible to even speak of a coherent 'blockchain industry' or 'community' in the

first place, and the kinds of politics that are being shaped through such a sensibility. I here introduce each of the cases, including Faircoin, to give an idea of how each of them enabled me to address my research questions.

Bitcoin: the invention of the blockchain

Bitcoin was first introduced in a post to the Cryptography mailing list by the anonymous Satoshi Nakamoto, who subsequently articulated the Bitcoin project into a concise whitepaper outlining its reasoning and design in a short nine-page document (Nakamoto, 2008).[18] The project was a proposal for a peer-to-peer electronic payment system, a transaction system without the need for trusted third parties to facilitate payments. There is a large body of work that discusses Bitcoin as a form of money, addressing questions of currency design, the nature of money and so on (cf. Roio, 2013; Robleh *et al*., 2014; Cheang, Rivoire and (eds.), 2015; Peters, Panayi and Chapelle, 2015; Vigna and Casey, 2015; Bjerg, 2016; Scott, 2018). My focus in this thesis is specifically on blockchain and I therefore treat the Bitcoin case primarily as the invention of this particular data verification and storage method that it comprises, rather than assess its appropriateness as 'money' *per se*. As I argue in chapters 4 and 5, however, the monetary and economic decisions and aspects of blockchain protocols cannot be so neatly separated from its data structure and computational approach, and so my research does also address these aspects of the cases. There is justification for such an approach in that the Bitcoin whitepaper itself has not a single reference to monetary or economic theories and so what arguably holds a blockchain assemblage together are primarily particular computational ideas, an observation that I expand on in Chapters 4 and 5 (Nakamoto, 2008; Nakamoto, Bridle and Brekke, 2019). The Bitcoin case study was intended to provide the backdrop to the two subsequent case studies; by understanding the 'original' blockchain, I would then be able to compare and analyse the ways other projects sought to differentiate from Bitcoin, pointing to moments of decision and deliberate differentiation, the case serving as a basis for answering each of my three research questions. Over the course of the analysis, the Bitcoin case instead became the main case in my thesis, a key point and project through which to understand how concepts and understandings from network computation became more broadly relevant, and in turn generalised and 'tokenised' (in the sense of integrating currencies as a core aspect of decentralised protocol design) as I discuss in Chapter 4 and 5.

Ethereum: generalisation of the consensus algorithm

Ethereum inventor Vitalik Buterin was one of the first to explicitly articulate and build 'blockchain' as significant in and of itself, and therefore as more than a proposal for

[18] See http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

decentralised electronic money.[19] Ethereum launched in 2014, some years after Bitcoin and after a period of 'alt-coins', which were experiments with different cryptocurrency designs in the wake of Bitcoin. The aim of Ethereum was to expand the remit of Bitcoin from being a decentralised payment system (the invention of 'cryptocurrencies') to a more general decentralised system able to handle any kind of application (reframing Bitcoin as the invention of 'blockchain'.) Ethereum in this sense also marked the expansion of the understanding and operationalisation of concepts in Bitcoin, the 'platformisation' of blockchain and decentralised protocols (see Chapter 5). I therefore chose the Ethereum case study with the intention of understanding the ways in which the specific assumptions, ideas and logic of the Bitcoin consensus algorithm were generalised to serve any kind of currency, protocol or application. This in turn, would address my first research question, making more evident some of the core ideas informing Bitcoin by building and expanding on these, as well as my second research question, pointing to some of the ways that concepts of decentralisation, trust, consensus and related concepts are operationalised. Because Ethereum launched as I was beginning my PhD research, I had the opportunity to follow the case as it developed, which also saw the project, developers and enthusiasts work through very fundamental questions about the ability to replace authority with code – culminating in a major conflict and 'fork' of the project towards the end of my empirical research. The question of the political re-emerged through these conflicts in the Ethereum community itself. As the research progressed, my third question, and methodological strategy of focusing on difference, disagreement and disputes (whether technical or otherwise) were both fully justified and served as a timely input to the debates at the time (outlined below).

Faircoin: political differentiation

I chose the third case study, namely Faircoin as it represented a deliberate and explicitly political differentiation from both Ethereum and Bitcoin, started by anarchist networks in Catalonia, Spain, in 2014.[20] The project was initiated and funded by the anarchist Enric Duran, who had escaped from Spain after publicly declaring that he had taken out loans from banks amounting to €500,000 between the years 2006-2008 that he was not intending to repay.[21] Instead, the money went to fund infrastructure, land and capacities of what was called the Cooperativa Integral Catalana (CIC), a cooperative network with the aim of an 'integral revolution' that would involve a transformation of the means to support 'all aspects of life', which also incorporated several local social currencies and bartering networks.[22] Through the CIC Duran in particular sought to politicise aspects of money, finance, accounting and taxation, not just in terms of critique of established processes and institutions,

[19] See *What is Ethereum* (2014) available from: http://youtu.be/Clw-qf1sUZg [accessed 24.03.2015]
[20] See https://fair-coin.org/
[21] See https://vimeo.com/darkoptimism/robinbank
[22] See https://cooperativa.cat/es/

but as a direct action strategy, also called 'tax disobedience'. When Duran escaped court by leaving Spain, he sought to expand many of the ideas of tax disobedience, financial, economic and political autonomy of the CIC, and FairCoin was launched under the organisational umbrella of FairCoop with the motivation to scale these initiatives to global scale – a global social currency for use amongst cooperatives across the world and under direct democratic control.

Many of the critiques of existing institutions and strategies of disobedience have significant and interesting overlaps with the cryptocurrency ecosystem more broadly, although the political reasoning varies significantly. The Faircoin project draws on explicitly social movement ideas of 'decentralisation' as well as consensus, trust and other major concepts in blockchain. The Faircoin project altered the Bitcoin consensus algorithm in order to correspond with ideas that prioritised direct democratic oversight over algorithmic processes, naming the 'global assembly' as the primary determining body. This reliance on assembly-based decision-making, and the mediums through which assemblies took place – which were a combination of Telegram group chats and online pads for note taking – suggested a different set of questions, theories and literature than were my primary concern in this thesis, and so have not been included in the empirical chapters. I include the case here, and discuss it briefly in the conclusion, because it nevertheless served as an important marker of differentiation during data-collection and in my analysis and therefore forms part of the analytical backdrop even if not explicitly discussed in the empirical chapters 4-6.

3.1.2 Ethics and positionality

Over the course of the research, I increasingly took the position of critical insider in the field, being invited to contribute to educational material and public debates about blockchain by people in the industry (see specifics below). Researching a field that I myself was becoming a participant in raises some ethical concerns and questions about positionality, transparency and the effects on the field I am researching as well as my findings. I briefly discuss these here before discussing the limitations of my research methods.

Issues of ethics and positionality, in particular when it comes to participatory methods, concern differences in power dynamics, questions of transparency and not causing harm (cf. *Community-based Participatory Research: Ethical Challenges*, 2011). In the case of my empirical work, the communities I was studying were mostly highly educated researchers and developers from technical backgrounds, themselves engaged in research. This meant that my position as a researcher was neither unusual nor a threat, but in fact welcomed by the communities and industry, in particular because of my social sciences angle on a technical field grappling with questions of power and radical reorganisation of economic, political and social processes. Furthermore, the blockchain community is one that is exceptionally aware

of issues of security, privacy and transparency, such that information and opinions are often radically open. Code, papers, opinions and interactions tend to be fully published, often leaked by the community itself; if, on the other hand, these contained sensitive data, this was made very clear to me and the documents were cryptographically secured. I was generally a bystander of such dynamics of hiding or revealing, witnessing as a chat log was published following the Ethereum DAO exploit for example (see Chapter 6). That is to say that I worked almost exclusively with data and information that were already made public, discussing personas and positions that were in the limelight already as public figures.

It is worth explicitly stating that Bitcoin, blockchain and cryptocurrencies are, as mentioned in the introduction, associated with and implicated in illicit and geo-politically contentious activities, markets, hacker cultures and politics, the 'Darknet' and so on. Had I addressed more practical case studies, for example hacker involvement or the uses of blockchain by political movements, there would have been significant questions, ethical and technical aspects to address – confidentiality and the security of identities in particular. However, my study has focused on people and places that are not currently under threat legally or personally, and draws almost exclusively on material that is already widely published and openly available online. When I engaged in more private conversation, it would usually be to seek verification or clarify details of online rumours. These conversations were neither recorded nor registered and do not form a substantial part of my data. For the few recordings and interviews that I did conduct, the usual ethics of seeking explicit consent apply.

In terms of access to the community itself, developer conferences and meet-ups were generally very open and inclusive spaces, making it easy to engage with. This earlier work, and the assistance of my colleagues in computer sciences, also gave me a means to check my technical understandings. Following an invitation by a blockchain developer training company, B9Lab, to write a 'Hippocratic oath' for blockchain developers, I became increasingly drawn in as a 'critical insider' in the field.[23] Where I had begun my research from the position of critique, sceptical of many of the projects I was looking at, in the empirical work I found that critique was generally welcomed and that many people were themselves openly grappling with questions and concerns about what they were building with blockchain. This realisation significantly impacted my research, interpretation and analysis. My approach increasingly became to, in the words of Haraway, 'stay with the trouble' (2016) and, in the words of Barad to 'meet the' (blockchain) 'halfway' (2007). I found that the developers, computer scientists and engineers were themselves grappling with the ways the technology might not be living up to claims made of it, and were correcting, building and addressing this. I wanted to take these efforts seriously, and instead of keeping at a safe distance, to contribute

[23] See https://www.b9lab.com/

my own critical work to this process of shaping the possibilities and directions of the field. Such an approach might be understood to compromise the 'objectivity' of the research: if I myself was beginning to have an active stake in how projects and debates in the industry developed, would this not in turn affect and potentially compromise the integrity of my findings? Furthermore, would it not also represent a conflict of interest? In reference to Barad's approach to 'objectivity', there is no 'outside'. An observer, and any description of the observed phenomenon will in turn affect its very determination. Indeed this is usually an ambition in research, to contribute to knowledge about a given field such that it can be understood and developed further. It becomes less important to construct a position of neutral outsider, and instead essential to articulate and explain the nature of the interest and stake in the field, the motivations behind the research, the ways in which the material and phenomena were engaged with and the reasons for the arguments made. My intention with this thesis is not only to go out and 'find' what matters politically in blockchain, but to take part in articulating this, and make the claim of what kinds of things matter as a contribution to a broader conversation. It is also important to state that this did not involve any direct material or financial stake: I did not at any point work directly for, or receive any remuneration from, any Bitcoin affiliated companies, nor from Ethereum. While B9Lab at the time of my work with them were offering Ethereum courses to developers, the work I conducted aimed to contribute to a critical reflection on the systems that developers build.[24] It is also worth stating that throughout the research period, I only held small amounts of bitcoin (the most I had at any one point was 1btc) and ether (2 ether) for research purposes, in order to test wallets, Smart Contracts and transaction systems and that I have not, as of writing, exchanged for other currencies.

3.2 Data collection and analysis

My empirical data gathering took place primarily between June 2015 and June 2017, and took the form of three phases with different methodologies. In the meantime, the blockchain field was rapidly changing and developing, and so strictly speaking, I continued to keep informed on more general tendencies and changes to the field throughout the writing phase from July 2017 – February 2019. To give an overview, the table below outlines the different phases as well as my aims, methods and results of each. I then describe in more detail these phases of my empirical work, the kinds of methods I employed and data I was gathering. I complete this

[24] My work can be viewed here: https://blog.b9lab.com/proposing-the-satoshi-oath-for-developers-69003cffb022. For full access to review the ethical course material that I wrote, please contact B9Lab.

section with a discussion of how I went about analysing the data, arriving at the structure of this thesis and its main arguments (see Table 1 below).

	Aims	Methods	Result
Phase 1: ***Sense-check***	Sense-checking case studies and blockchain as focus of the thesis.	Netnography (code repositories, online forums and blogs, email lists of case studies, chatlogs); Government and industry reports; Reporting in major media outlets.	The cases were considered significant, representing main projects in the industry and significant variation for comparative study.
Phase 2: ***Technical understanding***	Gaining and testing my technical understanding.	Reading whitepapers and technical literature; Practical use of Bitcoin, Ethereum and Faircoin, trying wallets, and transactions; Conducting interviews; Watching video archives of early cryptocurrency interviews.	I wrote several iterations of my own explanations of the architectures, and drafted glossaries.
Phase 3: ***verifying descriptions and understandings***	Sense-checking my own technical and conceptual understandings.	Writing educational material adopted by industry; Doing public presentations for technical and non-technical audiences related to the industry; Participating in technical seminars.	I was satisfied that my technical understanding had reached a sufficient level – verified by industry adopting my writing, and through the responses to my public presentations.

Table 1. Phases of data collection.

3.2.1 Empirical phase 1: sense-checking the cases

The aim of the first phase of the empirical research was to address the potential issues of studying a very new and emerging technology and sense-checking the selection of case-studies by ensuring that these had a) active developer communities, b) growth as projects and c) enough uptake and investment (financial and/or social) to assume ongoing development, at least in the medium term. This took place between June 2015 and June 2016. Ethereum had only recently launched, and their first developers' conference took place in the City of London just as I began fieldwork.[25] Faircoin had only just commenced with a first 'airdrop' distribution of coins a year earlier.[26] This phase also entailed getting a preliminary overview of where these projects sat in relation to the broader field of blockchain development to see whether there were more suitable cases or if indeed Bitcoin, Ethereum and Faircoin could be argued to represent a diversity of the field in general and meaningful differences in

[25] Ethereum DevCon 1, Gibson Hall, City of London November 2015 https://blog.ethereum.org/2015/09/24/devcon-is-back/
[26] See https://wiki.fair.coop/en:faircoin:start

development pathways more specifically. The methods I employed in in this first phase were primarily 'netnographic' (Kozinets, 2015) observation and following the online and offline communities of the different case studies, taking notes and writing observations (see Appendix for details). I approached the field largely through the lens of science and technology studies (STS) (Law, 2016). Inspired by Latour's use of multiple notebooks (Latour, 2005) I wrote extensive notes and used writing as a research method at the early empirical stage as a means to reflect on and articulate my observations in relation to my research questions. I also paid attention to more general media reporting on cryptocurrencies and blockchain as well as government and thinktank reports (Erb, 2015; Naughton, 2016; Walport, 2016). From this material, I concluded that the cases and 'blockchain' more generally were significant and likely to be long lasting enough to warrant further study.

It became clear that the field was rife with inflated claims of social and political transformation as well as new blockchain projects vying for attention. It was not always easy to tell what might be a 'scam' from longer-lasting, more serious projects, and whether claims were in any way pursued in actual technical development. To ground the research further and get a better understanding of the people, industries and investors involved I attended local meet-ups and gatherings, initially in London (see Appendix). These included, *Coinscrum*, a monthly meet-up for all types of cryptocurrency projects based in Shoreditch, London; the Robin Hood Coop 'office' in London August 2015, housing a hedge-fund coop with the idea of hacking the financial industry for social good; and the Tuttle meet-up in the City of London and social events in the cryptocurrency community. Between 2015 and 2017 there was a continuous stream of blockchain-related events, further proof of a growing institutional and business interest in the technology and what seemed like a positioning of London as a centre for the emerging FinTech industry more generally. These industry events helped give an idea of the types of actors interested in and working on blockchain, find out more about the aims and interests of investors in current blockchain development – in particular to understand what seemed to be a radical shift taking place from the early days of Bitcoin where the project was mostly associated with criminal activities and largely seen as undermining existing financial institutions to a new-found focus and hype on the blockchain as a piece of financial innovation for these very institutions.

After this first phase of data gathering I concluded that the selected cases had active communities who also, to a large degree, varied in their political aims and ambitions. Satisfied with the cases and the focus of the research overall, the next step was to ensure a deep understanding of the technical architectures of the three case study platforms in order to be able to distinguish claims from actual effects and be able to analyse the intentions and implications of their designs.

3.2.2 Empirical phase 2: technical understanding

The second phase of the empirical work partially overlapped with the first, with the most focused data gathering work occurring between November 2015 and June 2016. This phase involved immersing myself further in the field in order to a) familiarise myself with the applications by trying different wallets, using the cryptocurrencies and explore Smart Contracts; b) gain a deeper grasp of the technical architectures; and c) develop better understanding of the communities involved and the evolution of the industry. In order to ensure a good grasp of the technology, from a user perspective as well as its architecture and its rationale, I started my research of each case study with a thorough reading of their whitepapers – high level descriptions of the intention, purpose and core technical proposition of the currency. The methods I used in this phase involved researching the different clients, wallets, applications and currencies, reading technical papers and tracing in particular historical papers on cryptography in order to understand how it is employed in blockchain (see Appendix for details). I would then write up my own descriptions of the architectures in order to test my level of understanding at this point, which also became an exercise in translation. This process brought up an issue of slippage of meaning between technical terminology and socio-political practices, both by myself and in the manner in which the applications were presented; for example, with the notion of 'decentralised consensus', referring to a computational problem that simultaneously presented a tempting socio-political proposition. The awareness of such slippages informed my observations and questions in interviews and at events. I conducted a number of semi-structured interviews (see Appendix). As it turned out, most of these repeated information and attitudes that were already evident and available in online videos, posts and discussions. This was likely due to the timing of the interviews in early-to-mid 2016 when the industry was experiencing a boom, making it difficult to move beyond the surface of excitement and selling of ideas. On the one hand the interviews thereby served to confirm coherence between information and attitudes expressed in online material, but also meant that I took the decision to draw on such online material as a primary source rather than seek out further interviews (see Appendix). Had the interviews taken place a year later, during and after some of the major forks and disputes in the community, and had my own understanding of the field and the stakes reached a sufficient level, the interviews might have been more focused and insightful. Regardless, a large part of discussions and activity in blockchain takes place online, and the community has a culture of openness and leaking, so there was plenty of available data to work through. I drew heavily on these resources, in particular on the work by filmmaker Tomer Kantor and the IamSatoshi production team who had been extensively documenting and interviewing key figures and developments in blockchain from the early years.[27]

[27] See https://www.youtube.com/results?search_query=IamSatoshi and Ulterior Motives interviews by Tomer Kantor.

During this period Bitcoin was going through a prolonged conflict over a fundamental change to the protocol, which also signified a potential change to the governance structure of the currency. Instead of having to rummage around the Bitcoin GitHub repository on my own trying and draw out issues of governance and power, these events brought such questions immediately to the foreground.[28] I traced the conflict across discussion boards, email lists and news outlets, writing and rewriting descriptions of the conflict (see Appendix). Discussions oscillated between technical, ethical and political concerns, bringing out questions around technological determinism and the impetus and assumptions that drive and shape development pathways. It also became clear that there were fractions and interests in Bitcoin that I was not able to fully grasp. In the case of Bitcoin and Ethereum, the plethora of information, sites, blogs, rumours and claims online proved tricky, so I initially relied on informal conversation with contacts in the industry (explained in ethics and positionality above) to verify rumours. In the case of Faircoin, online documentation was fairly opaque. The project was based more on assemblies, the chat application Telegram and trusted networks. In order to get a fuller understanding of the cooperative movement context and actual usage of the currency on a day-to-day basis, I undertook three field trips to Catalonia and one to Athens over the course of 2016 (see Appendix).

To get a better understanding of Faircoin, I stepped away from the explicitly FinTech and start-up-oriented events and started tracing the political alternatives being developed. I took part in seminars with social currency networks and the city of Barcelona, which also had attendance by local Bitcoin entrepreneurs as well as a cryptocurrency ATM hardware company. I omit the details of these seminars here in part because my thesis no longer addresses Faircoin, social currencies and the Catalan case explicitly, and therefore will not be able to contextualise these seminars in an adequate manner. It is worth mentioning, however, because conversations with the ATM hardware company in particular were very revealing with regards to the amount of practical and logistical work that was being put in to establishing infrastructure for international currency circulation even under conditions of extreme legal uncertainty. I traced the Faircoin infrastructure and project through two more field trips, including a location where Faircoin founder Enric Duran was in exile. Apart from interviews with Duran and other core Faircoin developers I also visited the Faircoin project spaces *Aurea Social* in Barcelona, the local and very active Girona Faircoin node towards the end of 2016 and the offices of a Bitcoin ATM company operating in the Mediterranean. These visits gave a good insight into the enthusiasm and energy that infused the projects at the time where technical and legal architectures were being rapidly built and deployed regardless of their legal standing and uses. This seemed to cut across all cases, and also showed how the difference between what might be considered a 'scam' or simply mismanagement due to

[28] A series of in-depth articles published in *Coindesk* by researcher Aaron Von Wirdum in particular helped for understanding the stakes of various actors and potential outcomes (2015a, 2015b, 2015c, 2016a, 2016b, 2016c).

overambitious and enthusiastic ideas, development and experimentation was largely a matter of perspective – all projects operating in a legal grey zone. My grasp of the technical aspects of each project and the ways in which I sought to relate them to issues of governance and power still seemed untested and indeed my own role as a researcher within this field remained vague. So, in the third phase of the empirical research, I focused on publicly verifying my understandings of the cases and the ways in which I was translating these by taking part in events, presenting my research and observing how these might be received in the field.

3.2.3 Empirical phase 3: verifying descriptions and findings

Overlapping with my research of the technical architectures, the aim of the third phase was to translate and validate my own understanding of the technologies by standing up to scrutiny in the field. To do this I became involved in the work of B9Lab, a company providing online training, talks and intensive workshops on Ethereum for developers as well as business people. With one of the first structured Blockchain training programs, the company sought to set the standards for the industry, and invited me to develop their ethical training module and a 'hippocratic oath' for developers.[29] This allowed me to think through and test how the Ethereum community conceived of ethics, social relations and power in relation to the blockchain. Events surpassed my efforts in drawing out and making questions of power relevant to a technical audience: a major Ethereum-based project, The DAO, had been hacked for $60 million, throwing doubts on claims of neutral technology free from the intervention of potentially corrupt humans. Ethereum developers were forced to intervene, and decided to implement what is called a *hard fork* (splitting the Ethereum blockchain, see chapter 6) to cancel the hack, causing much controversy in the community and throwing up questions of governance and power in the process. I followed the hard fork closely and discussed the issues at stake with Ethereum developer Vlad Zamfir on the day it was taking place.

I also held a number of public presentations for different types of audiences to begin to get feedback on my ideas. Initially at *Re:Publica* in Berlin, May 2016 (in collaboration with Elias Haase of B9Lab, and including a meet-up on Blockchain and governance), at the *Nau Bostik* cultural centre in Barcelona November 2016, at *MediaLab Prado* Madrid, November 2016 (as part of a hackathon on *Collective Intelligence for Democracy*) and a growing number of these.[30] [31] While the different events had quite different audiences, ranging from professionals

[29] See https://blog.b9lab.com/proposing-the-satoshi-oath-for-developers-69003cffb022

[30] See: https://re-publica.com/16/session/blockchain-crash-course-and-challenging-consensus and http://16.re-publica.de/en/16/session/blockchain-meet. Re:Publica also hosted a second session on blockchain and governance by Shermin Voshmgir, also very highly attended.

[31] See: http://medialab-prado.es/article/madrid-inteligencia-colectiva-para-la-democracia. Documentation here: https://youtu.be/0acyX7SlfME

in the broader field of technology (Re:Publica) to a mostly anarchist audience (Nau Bostik, Barcelona), all of them included people who had a deep involvement with cryptocurrencies as well as people entirely new to the field. My reasoning was that if I could explain the architecture to a new audience while not insulting those with strong technical backgrounds, I could safely assume that I had reached a sufficient understanding of the technologies to proceed with a rigorous analysis of governance and power. Indeed, the more blockchain-aware people at the presentations were not only satisfied with the explanations I provided but were appreciative of a rearticulation of such architectures from the perspective of power and governance. The need for some contribution from social sciences to the field was generally widespread, possibly in part because of the backdrop of ongoing Bitcoin scaling conflict. I further verified and expanded my technical understanding by attending the mostly academic Bitcoin Summer School in Corfu, Greece, organised by the International Association for Cryptologic Research and UCL Computer Science department. Two insights in particular were gained from this: firstly, a hint of what was going to become the field of 'cryptoeconomics' as I saw computer scientists discuss economic theory as part of their computational models in a presentation by Aggelos Kiayisas of the School of Informatics at the University of Edinburgh; and secondly, the specificity of ideas and aims of decentralisation in technical field, in particular through presentations and insights by Sarah Meiklejohn and George Danezis from the Computer Engineering department at UCL (see also Troncoso *et al*., 2017; Meiklejohn, 2018).

3.2.4 Data analysis

Throughout my data gathering, I had been writing and rewriting descriptions of the architectures, observations, difficulties and contradictions in the field, inspired by Latour's method of keeping several notebooks (Latour, 2005); one for documenting the research process, one for observations that might be thematically organised, one for 'writing trials' testing different articulations and a final notebook to log how such articulations in turn would affect the context and people involved. Although my own writing practice has admittedly not proven so consistently and neatly organised, this method of separating out different types of writing and thinking exercises proved very useful for tracing through the field work and material. This practice also came to form a large part of my method of analysis, writing up how I was reasoning with the field, with public presentations continuing to serve as a way to further shape and test my analysis as I went along.

During the fieldwork I developed and worked with a conception of three 'layers' in blockchain technology that, informed by my theoretical research, seemed to form different ways in which power and the political played out, namely *protocol*, *governance* and *interfaces*. The *protocol* layer would refer to the 'technology' of blockchain proper, implying an encoded politics that

would execute in an immanent manner, and which suggested that my task as a critical researcher was to reveal such a 'hidden' technological and infrastructural politics. The *governance* layer referred to the writing and governance of such protocols, in the form of the more explicitly politicised negotiations that were taking place in conflicts over protocol development in Bitcoin and Ethereum. My task as a critical researcher at this layer would be to lay bare the power dynamics at stake in the governance methods used for decentralised protocols. Finally *interfaces* implied the ways in which 'the political' in terms of actual effects always played out in relation to other contexts and conditions. Here, I understood my task as a researcher to be to highlight these often overlooked contingent political effects and articulate the importance of such contingency for understanding the political effects of blockchain. These layers served as helpful ways to focus the research, but in further analysis some of the assumptions underpinning these proved tricky and opened up new questions. The main issue I came to face in my analysis was how to define and address the 'object' of study more precisely.

The object of my study was supposed to be 'blockchain', and my research questions were aimed at understanding the political implications of this object. But 'blockchain' in the meantime proved less contained than anticipated, operating in and through mediums, papers, promotion, code, ideas and attitudes that were not strictly limited to a technical coherent 'thing'. Those things that might be considered closest to the technical object of 'blockchain', such as the Bitcoin reference client for example, were themselves even up for dispute (see chapter 6); the Bitcoin reference client proved to be an unstable thing that would be updated, 'forked' and run in different iterations and hardware, across various networks. This proved tricky in writing, then, because any description of 'blockchain' had to be qualified: was this a description of blockchain in its ideal form as written in the Bitcoin whitepaper, or did it describe how the network actually currently operated? Or would a description as it was experienced by different parts of the system, promoted, attempted legislated be more useful? From whose perspective was I speaking, and what purpose were my descriptions trying to serve? I struggled to avoid simply repeating the plethora of online descriptions of blockchain, as I was only too aware that these descriptions were not capturing the complexity of how both the idea and the technology of blockchain operated – but these nevertheless were important in themselves. In order to work through the entangled data, perspectives, observations and material developments, I developed and drew up tables to articulate my own distinctions in what was taking place – comparing use of concepts as discussed above ('decentralisation', 'trust', 'consensus' and so on); comparing descriptions of applications to my own experiences of using these and broader reported effects; and comparing cases and changes to protocols and attitudes internally in projects over time – what I came to understand through Barad as onto-epistemological 'cuts' (Barad, 2007).

The issue of a non-stable object led me to describe a 'sensibility' rather than a thing, an emerging attitude of assumed 'good' and 'bad', 'desirable' and 'undesirable' that informed the field and the development of new projects and were common across all cases. The most obvious of which was 'decentralisation' as good and desirable and 'centralisation' as bad and undesirable. My use of the word 'sensibility' to describe these attitudes worked for two important reasons; firstly, because the term captures a general common sense rather than something more coherent such as a definitive 'politics of blockchain', for example, which simply did not ring true; and secondly, because it nevertheless did tie into ideas of political theorist Rancière, who describes *the political* as exactly a moment of disruption and redistribution of the sensible – namely a redistribution of what is commonly understood to matter. The term sensibility therefore proved helpful for understanding the particular form of disruption that blockchain presented, and to point to a moment of *the political*, a shift in what was considered to matter, while not assuming or demanding a definitive 'politics'.

Conceptually, working with ideas of sensibilities and sensing apparatuses tied in neatly with the onto-epistemology of Karen Barad (Barad, 2007). The ways in which sensing apparatuses, and indeed sensing agencies more broadly – whether human, technical or otherwise – are part of determining matters lent a certain acknowledgement to the deterministic aspects of systems designs, while simultaneously insisting on the limits to such determinacy (discussed at length in Chapters 2 and 4). Kathryn Yusoff's theoretical articulation of the insensible in relation to the political then allowed me to shift my analysis of the protocols, instead of attempting to grasp complete coherence and knowledge of the stakes of a given design to instead understand this as the very condition of their development (Yusoff, 2013a). The 'insensible' then would be those unknown contingencies as well as that which has not been factored into the model but which nevertheless is understood to exist. I then developed my concept of the *dissensible*, drawing on political theorist Rancière (Rancière, 2010), as a means to describe the ongoing possibility of incompatible sensibilities, as a way to analyse the political in relation to a technology that claims to solve it. I developed a table as a means for organizing these three conceptual approaches, their theoretical scope and main questions in relation to the empirical material. I made consistent use of this table and, with these three 'cuts' in mind I went back over the empirical material. This table also came to inform the structure of my chapters:

Agential realism	Insensible A politics of matter	Sensible How things come to matter	Dissensible Resolving incompatible mattering
The political	The political as insensible, immanent and protocological	The political as a redistribution of the sensible/ possible	The political as dissensible, emerging incompatible difference
Questions raised in the cases by these definitions of the political	How is this political proposition sought encoded, materialised and enacted? What is excluded in its determination?	How did blockchain come to matter politically?	How does the assemblage deal with mutually exclusive positions? How is dissensus resolved in the assemblage? What holds the assemblage together?
Questions raised in the cases through this literature	What are the deterministic limits of protocols? How can an immanent politics be understood when its implications are emergent and not necessarily fully visible/knowable? How does the protocol deal with indeterminacy and the insensible?	What are some of the ways that blockchain applications relate to other economies, systems and spaces? How are these relations understood, politically? How do these relations play out politically?	How is the political reconfigured in relation to 'post-political' protocols? What becomes the new legitimate mode of conducting politics?

Table 2. Conceptual 'cuts' on the political and main questions asked of the empirical material.

3.3 Conclusions and methodological limitations

In this chapter I described and discussed my methodological design, its implementation and how I went about analysing my data. I took a case study approach for the methodological design, drawing on mixed methods in order to trace through answers to my research questions in each of the cases. This involved a combination of 'netnographic' research, ethnographic observations, a limited number of interviews, writing as method and tracing through concepts across technical papers, promotional material and online discussions. I also

used my own public presentations as method for verifying my understandings and testing my arguments, in particular in relation to my technical understanding. The cases enabled me to go in-depth in my understanding of the technical architectures and the culture around their development. The Bitcoin and Ethereum cases were selected on the basis of being the two largest blockchain networks. In my further analysis, I take this to mean that these cases set much of the standard not only technically but also in terms of 'sensibility' for the rest of the blockchain industry. This is, to some degree, an assumption. Nevertheless, the two cases remain the largest blockchain networks. They form two important moments in the history of decentralised network technologies, such that recounting their particularities and histories are important in their own right, having opened up new fields of computation. To conclude the chapter, I briefly discuss some of the limitations to my approach and methodological design, some alternative approaches and the reasons why I did not pursue such alternatives.

3.3.1 Methodological limitations

My initial assumption, that the political implications of the technology and site of decision-making would be defined in and through protocol development, meant that my focus was primarily on the protocols and developer communities, rather than deployment and effects amongst people using the applications and technologies. This initial assumption brought with it significant analytical limitations and certain biases, the most important of which is that I thereby risked reproducing in my own work a certain technological determinacy that was very much present in the blockchain industry more generally: that what matters primarily is the protocol and the ways in which it determines things. An alternative approach to 'the political' in relation to blockchain might therefore have been to address the deployment and uses of the technologies, which might have been a more powerful angle from which to assess claims made of it – comparing claims with substantial research into its uses and effects in different contexts. Such approaches, however, have already been the focus of many critics of blockchain, and tend to produce analyses concerned primarily with disproving the claims and efficacy of the technology (O'Dwyer, 2015; Golumbia, 2016; Gerard, 2017; Vidan and Lehdonvirta, 2018). I wanted to address blockchain from a more open perspective, to meet the claims 'halfway' to paraphrase Barad (from the title of her book, 2007), in order to understand its merits and contribute to an articulation of what might be possible. In other words, instead of claiming that it is either 'right' or 'wrong' or 'works' or doesn't 'work', I aim to understand in what sense it does or does not work, and how and why it is corrected for. I aimed for an approach that would be more open to the possibilities in the space, what is at stake in their materialisation and how this might be articulated and therefore shaped more clearly.

At a certain point in my analysis, however, I had to step 'outside' of the protocol so to speak, to be able to understand how its descriptions operated politically in themselves. This represented another analytical angle that critics have effectively employed for analysing blockchain, namely to address how blockchain operates as a narrative device, more effective as a story about money and power, than a technique, tool or technology (Golumbia, 2016; Reijers and Coeckelbergh, 2016; Kreutler, 2018). Such an angle might have benefited from a systematic discourse analysis in the field, but instead I opted to trace the use of concepts through histories of cryptographic and computational advancements, alongside forum posts and discussions, essays and commentary on Medium (an online publishing platform on which major actors in the industry tend to publish their reflections), mailing lists and technical papers. I did this because I did not want to emphasise a distinction between discourse (claims) and materiality (reality), but instead to understand how historical experiences, technical papers and networks played into each other and were entangled – an onto-epistemological approach so to speak, whereby discussions feed into experimentation, changes to designs and ideas about the world. My hesitation was that discourse analysis, by overly focusing on words and ideology, might lend itself to the assumption that something else is happening in 'reality' while the discourse operates as a set of false claims or dubious ideology. Precisely because 'Bitcoin is a technology whose social and political functions far outstrip its technical ones' (Golumbia, 2015, p. 119), these would need to be addressed as part of the motivating factors as these social and political functions fed into ongoing efforts to materialise new technical architectures and resonated with experiences, projects and ideas across different contexts.

Another alternative research design to understand some of the political implications of blockchain might have been to 'follow the money' so to speak, and analyse the specific individuals, companies and investment flows to achieve a map of different kinds of stakes and interests in systems being developed. This would have been a fruitful approach for analysing, in particular, the disputes around protocol changes that were playing out in the case studies (discussed in chapter 6) and gaining an understanding of who might have a stake in different kinds of outcomes. This approach might have given a good overview of the relationships, interests and stakes, but at the time did not seem an effective approach for gaining a deeper understanding of the political ideas and sensibilities that were forming and informing the assemblages. Such a social and value network analysis would be hugely valuable, but was beyond the scope of this thesis due to time limitations and the labour-intensive nature of such a mapping endeavour.

The next three chapters form my three Baradian 'cuts' in the blockchain field. Chapter 4 addresses the technical architectures of Bitcoin and Ethereum and their analysis in relation to the indeterminate and *insensible*. Chapter 5 traces the pre-histories of these architectures in

previous generations of decentralised architectures to understand the particularities of a blockchain *sensibility*. Situating Bitcoin and Ethereum in such a historical trajectory of decentralisation also allows for an analysis of what has changed with their invention, namely the platformisation of decentralisation and 'tokenisation' of protocols, the implications of which I discuss in this chapter. Chapter 6 describes two major conflicts in Bitcoin and Ethereum. I introduce the concept of the *dissensible* through which to discuss the ongoing possibility for things to be different and for these differences to be incompatible. The chapter discusses issues of dissesus over the governance of protocols that were supposed to have solved the problem of consensus and a resolution to this through 'forking' that I discuss as a 'dissensus mechanism'.

4 A Politics for the Insensible

> … a kind of affirmative action for the formless.
>
> – Yusoff, 2013a, p. 224

In this chapter I describe and analyse the Bitcoin and Ethereum protocols and how the techniques and technologies that form their architectures, specifically cryptographic proofs and decentralised networks, become the foundation for broader claims and perspectives on the political. I address and analyse the intentions of determining trust, truth and certainty through cryptographic proofs, and bring in the notion of the insensible to shift the ground of debate from a competition between humans and machines to a question of affinities. The chapter is structured as follows: I first explain some basics of cryptographic hashing and describe how cryptographic proofs are used in the Bitcoin architecture with the aim of eliminating the need for 'trust'. I describe how trust is understood and operationalised in very specific ways in Bitcoin and decentralised network security, and the particular kinds of determinacy that these give rise to, before discussing the limits to this form of determinacy and the ways in which the network has emergent effects in ways that require contined correction and maintenance. I draw on Barad's understandings of determinacy as enacted in and through different forms of agency in order to do so. In the second half of the chapter I then outline how the elements that make up Bitcoin are extended in the Ethereum platform with the aim of developing a generalised platform. This also extends ideas of a trustless system towards ideas of an autonomous system necessarily operating beyond human control, lending the system itself certain agency. I discuss some of the issues of the extension of algorithmic determinacy on the basis of an assumed universality of cryptographic proofs and decentralisation, suggesting a re-reading of such determining agency through ideas of animism. Instead, affiliations that cross human and otherwise are acknowledged, making the question not one of which is the most appropriate determining agency, human or machine, but rather what are the motivations for the necessity of an expanding algorithimic determinacy in this particular case. I conclude the chapter by arguing for a politics for the insensible, as both that which has not *yet* made itself matter, a moment before a political contestation of sensibilities, but also, and importantly, that which might never make itself matter, a beyond political contestation (Yusoff, 2013a).

I use the concepts 'determinacy', 'technological determinism', 'algorithmic determining agency' and 'determinate' repeatedly in this chapter, refering to slightly different but interrelated definitions which are worth highlighting here. Determinacy in terms of systems designs means a design for which a certain outcome can be determined. This is the promise of cryptography, which becomes the foundation for a broader technological determinacy,

whereby certain technological developments are assumed to be necessary, natural or innevitable. I address and critique this second notion of determinacy through a Baradian materialist understanding of how things are determined, namely in a quantum sense as determining the state of a phenomenon which might otherwise exist as an indeterminate potential state. My argument is that the determinate properties in specific systems designs (cryptographic proofs in this case) is the foundation for a form of technological determinacy that argues for the necessity or even inevitability of an algorithmic determining agency on the basis of it being a more objective medium for determining matters. I counter the necessity of such technological determinism without having to thereby also negate the determinate properties of cryptography. Drawing on Barad, then, the determinate properties of cryptography form just one particular way of determining things, with very particular effects. What makes it 'objective' is simply the fact that the conditions for its reproduction can be precisely conveyed and enacted. Yusoff's notion of the *insensible* suggests very real limitations to any determining sensibility by bringing awareness to the insensible, and thereby the impossibility of any given sensibility to fully determine or know what matters. What matters, and what is made to matter, becomes a question of affiliations rather than a universal registry. This makes the possibility of an algorithmic determining agency real, but also very situated – a project for and about the affiliations and desires of specific people seeking to realise such an agency, rather than a universal objective necessity.

Before commencing, it is worth restating that the specific technical developments in blockchain move fast and so aspects of the description might be slightly outdated – the consensus protocol used in Ethereum, for example, is intended to change from the proof-of-work protocol in Bitcoin to what is called proof-of-stake, presenting new design and conceptual challenges (some of which are discussed in 5.2.2). The technical descriptions are mostly high-level, however, and the main characteristics of the Bitcoin consensus algorithm are likely to remain as a standard from which other algorithms differentiate. The main intention of this chapter is to describe the ways in which the technical architectures form and inform conceptions of the political, rather than a description of the state of development and capacities of 'blockchain'.

4.1 Replacing authority with cryptographic proofs

> In words from history, let us speak no more of faith in man, but bind him down from mischief by the chains of cryptography.[32]
>
> – Edward Snowden, quoted in Greenwald, 2014, p. 24
>
> What is needed is an electronic payment system based on cryptographic proof instead of trust.
>
> – Nakamoto, 2008, p. 1

The main proposition of Bitcoin is to replace the 'authority' needed for running current payment systems to function with cryptographic proofs. Cryptography is a powerful tool that, as opposed to, for example, the law or armies, does not require many resources to operate. It is an 'asymmetric' technology (Buterin, 2016a), and as such has inspired ideas of resisting and holding accountable powerful actors, to 'bind him down from mischief by the chains of cryptography' as whistle-blower Edward Snowden proposes in the quote above. The comment is a reformulation of a historical quote about the US constitution by Thomas Jefferson and is telling of the ways in which cryptography, and the idea of code as an immediately executing language (code as law), is understood as a more powerful means for enforcing fairness, addressing power and the corruptibility of humans. It also shows that using cryptography as a means to counter authorities is not unique to Bitcoin but part of broader Cypherpunk, hacker and InfoSec digital cultures. Bitcoin and blockchain are developments of such ideas of establishing a neutral and incorruptible governing apparatus that would hold authority in check. What did, however, turn out to be unique in Bitcoin and blockchain were the ways in which these ideas became generalised and turned into a proposition for not only enforcing transparency and protecting privacy against authorities, but to replace authorities entirely. It is the reason for why, for example, an enthusiast at a London Bitcoin meet-up in late 2014 explained to me 'I don't believe in politicians – but I believe in maths'.

In the following, I describe some of the basics of cryptographic proofs and the ways in which it is used in Bitcoin to resolve the need for authority and then give an overview of the Bitcoin architecture and protocol. I then discuss some of the contradictions and difficulties of its implementation and how, by drawing a cut separating this 'perfect thing' from necessarily corruptible 'mushy humans', what I argue to be a form of systems primacy emerges whereby these can be sidelined as an unfortunate effect of imperfect humans. It is only by drawing that cut that the system can be construed as being beyond the control of humans, while long hours of human work, knowledge and effort are put into making it a reality. I then discuss

[32] Snowden is reformulating a quote of Thomas Jefferson: 'In questions of power then, let no more be heard of confidence in man but bind him down from mischief by the chains of the Constitution.

ways in which the *insensible* comes to haunt the certainty of cryptographic proofs through an awareness of the limits to what can be determined and known through and in the protocol. This then lays the ground for the next half of the chapter, which describes the Ethereum project as a generalisation of Bitcoin expanding on ideas of autonomy, trustlessness and decentralisation to form a kind of algorithmic animism.

4.1.1 Cryptographic proofs in Bitcoin

Cryptographic proof is the ability to prove something with mathematical certainty. It is a set of techniques and algorithms that take advantage of a particular mathematical phenomenon called **hashing**, whereby some data, when run through an algorithm, will produce a string of characters unique to that data. It is highly unlikely, *probabilistically* unlikely, that any other data will produce that same output when run through that hashing algorithm.[33] What this means is that the integrity of a given record can be cryptographically verified; if anyone has tampered with it this can be checked by running the data through the same hashing algorithm to see if the output is different. This is what is meant in the whitepaper by an electronic system based on 'cryptographic proof instead of trust'. The integrity of the data is verified through mathematical probability rather than trusting an authority or someone's word for it. Add a timestamp and it can be proven when a given record was made. Hash these together in a 'chain' or a 'tree' by referring to a hash output of a previous record, and you have a linear history of provably secure records, of, for example, Bitcoin transactions.

Cryptographic proofs are used widely and have come to serve a variety of data security and authentication functions used across several industries for the integrity of digital records and information. Research and development of new hashing algorithms has been ongoing since the late 1970s, developing new algorithms and functions with different properties and security models (cf. Merkle, 1979, 1982; Preneel, 2010).[34] [35] It is the basis of things like **public key**

[33] The exact probability, and hence certainty, depends on the hashing algorithm that is used. The likelihood of two different messages producing the same hashed output is highly unlikely (these events are called 'collisions'). SHA1 (Secure Hash Algorithm 1) was a cryptographic hashing algorithm developed and published by NIST (National Institute fro Standards and Technology, USA) in 1995, but research in the early 2000s led to higher plausibility of collisions (Preneel, 2010). 'This shows that for long term collision resistance (10 years or more), a hash result of 192 or 256 bits is required.' (Preneel 2010:2). SHA1 produces a 160bit output (for example, hashing the file test.rtf returns 4ceb6c436b0c7a8f279233e65492786a24b43e5d), so to increase security, NIST published three new hash functions (Preneel, 2010:6), amongst others SHA-256 which produces a 256bit output (in which that same test.rtf file would return f0a9dba07065d989cb3b6e1e2bc1bbd48a2844e7dc1192a76e81a901aaf1de0d). See 2007-2012 NIST (National Institute of Standards and Technology) SHA-3 competition for developing a new set of cryptographic functions.

[34] Even cryptographic hashing, while frequently assumed to be bulletproof, requires constant upgrading and maintenance in order to remain secure as computational capacity increases and new attack vectors are found. While larger size outputs are more secure because the likelihood of a different data input outputting the same string (what is called 'collisons) with a diminishing likelihood of finding collisions, they are also more expensive to compute. Bitcoin uses the SHA-256 cryptographic hash function, making it extremely unlikely that a 'collision' would happen. Given that even a slightest change to a message would produce a different output when hashed (unless in the highly unlikely event of a collision), the hashing function is a way to verify data integrity and ensure that a message has not been tampered with.

cryptography, **Merkle trees** and **digital signatures,** each of which are used in Bitcoin and many cryptocurrencies. Public key cryptography ensures that a message cannot be intercepted and is read only by its intended recipient. Here, cryptographic hashing is used to create a set of keys: one that can encrypt (a **public key**) and another that can decrypt (a **private key** that is kept secret). A person can share their public key with the world, so that anyone can write a message and lock (encrypt) it with their public key, meaning that it cannot be read. Only they (or someone in possession of their private key) can unlock, decrypt and read that message. The public key encrypts messages to be sent to the owner; the owner then uses the private key to decrypt messages. In digital payments, transactions are messages, and so for Bitcoin, public key cryptography is used as a way to determine ownership of a given message.

Cryptographic keys are also used for digital signatures, so that it can be proven that a message has been sent by a given source. The network can then verify that the transaction is indeed coming from the correct 'owner', by checking the signature against a public key. Only a person with the correct keys is accepted as having sent that message, or 'spent' that transaction.

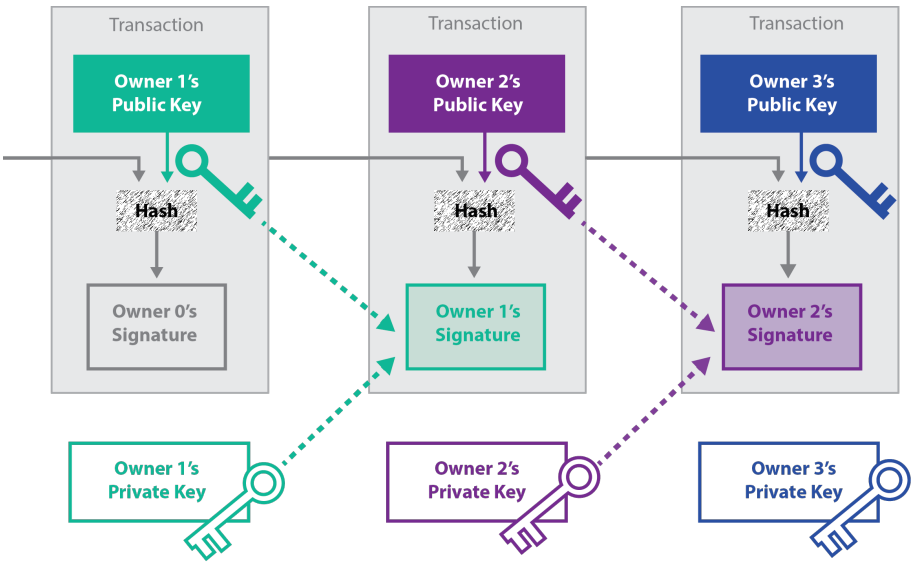

Figure 1. An illustrated version of Nakamoto's diagram of bitcoin transactions, 2008. Each transaction 'output' is linked to a previous transaction 'input' by the owner(0) signing the transaction data as well as the public key of the new owner(1) associated with a specific address and timestamping it.[36]

[35] Ralph Charles Merkle's 1979 *Secrecy, Authentication and Public Key Systems* report gives a very good outline of several basic concepts used in cryptography, including public key encryption, the use of these for digital signatures, and storing data in trees as an alternative form of verification to public keys.
[36] A good analogy is to think of this as an email address for money, you can have as many of them as you like, and they are not necessarily linked to your identity.

Rather than an actual coin, a bitcoin can be more accurately described as a chain, proving changing owners and records of accounts. Each transaction (output) refers back to a **digital signature** of where that value came from (the previous transaction input). In this sense, 'We define an electronic coin as a chain of digital signatures' (Nakamoto, 2008, p. 2). Transactions are thereby spent by unlocking funds associated with a given **address** using a private key associated with the public key that was hashed and signed by the previous owner; the next owner is determined by the current owner signing and hashing the public key of the person they want to send to. In other words, bitcoins are not self-contained 'coins' exactly, but rather a chain of spent and unspent transactions associated by signature with various **addresses** (see illustration above); a chain of transaction data that reaches all the way back to January 2009 when the very first transaction took place.[37] Cryptography is here once again used as proof – this time of ownership, using cryptographic keys, but also, and importantly, as proof that a given value spent in a transaction is genuine by proving its history through a public record of previous transactions. Transactions are thereby authorised through cryptographic keys, the hashed chain of transactions proves that the 'coin' comes from a valid source.

So far then, cryptographic proofs are used to ensure the integrity of a record of transactions, can prove and secure ownership through public key cryptography and can prove transactions are coming from the correct source using digital signatures. But the main aim of Bitcoin is to replace the need to trust in any authority, third party or intermediary with a peer-to-peer trustless network. This means that all this also needs to take place in a decentralised manner, such that no single 'authority' holds this record of changing ownership. Decentralisation presents some complications in terms of systems designs, and in order to solve these Nakamoto drew together an unusual combination of ideas. Instead of a bank, payments company or other 'authority' holding the balances of accounts and records of transactions, the intention is that these are held, verified and enforced across the peer-to-peer network – otherwise a centralised node would simply act as a new trusted intermediary. It is a conception of decentralisation that is operationalised as a means to eliminate 'trust', which in turn is understood as a security weakness, an unnecessary cost and a potential uncertainty by introducing the possibility of reversing transactions:

> Commerce on the internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions,

[37] The Bitcoin blockchain can be browsed using various 'blockchain explorers'. Here is a link to the details of the first bitcoin transaction between Satoshi Nakamoto and Hal Finney, an active contributor to the Cypherpunk email list: https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

> and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services.
>
> – Nakamoto, 2008, p. 1

The way that 'trust' and 'trustlessness' are understood and operationalised here is very specific and has its roots in both Cypherpunk culture and network engineering (see Chapter 5). The aim is to achieve a 'trustless' system for reasons of security: if a peer-to-peer network relies on any single node this opens up a security risk if that node happens to be malicious.[38] Mediation, as described by Nakamoto above, implies the possibility of reversibility and thereby uncertainty, and is assumed to also imply and extra cost. And so, in order to eliminate trust and intermediaries, instead of a bank or a third party registering and enforcing transactions, these are broadcast publicly to the network, which then witnesses them, checks their integrity and adds them to what is called a **Merkle tree** – a 'tree' of cryptographic hashes.[39]

There are some problems, or to put it in the language of network engineers, *attack vectors*, that are particular to developing a decentralised payment network. These are important to trace through, not only to explain the reasons for the Bitcoin protocol design, but also because the very politics of different design considerations tend to be discussed and addressed in network security terms. The ways in which these different attacks were solved would, in turn, end up having significant political and economic effects in the field of blockchain and decentralised systems designs. One type of attack that is common to decentralised systems more generally is the DDoS attack (Distributed Denial of Service attack) describing the type of attack whereby a network is spammed in such a way to make it unusable. In the case of Bitcoin, such an attack could, for example, consist of someone sending many small transactions to overload the network. In order to prevent this kind of attack, Nakamoto drew on work done by cryptographer Adam Back in an earlier project called Hashcash, which predated Bitcoin (Back, 2002).

Hashcash was a system based on research by Cynthia Dwork and Moni Naor in 1992, which suggested using computational difficulty as a means to combat email spam (Dwork and Naor, 1992). The idea was that by making it computationally expensive to send emails, it would discourage spammers from abusing the network. Back developed this idea into Hashcash,

[38] A trustless system is therefore a system in which a network needs to assume that not all nodes can be trusted. Networks are never 100% trustless. It can be assessed pretty accurately what percentage of the network needs to be 'honest', meaning interacting in the network in the expected and accepted ways, in order for it to work. A trustless system is one that is designed in such a way that even if there are malicious actors, misinformation or other issues, the system's integrity is maintained.

[39] A Merkle tree is an early form of hash tables, which are used in cryptocurrencies and decentralised systems that have come after Bitcoin in so-called distributed hash tables (DHT). This is a method of effectively storing and retrieving data across a network.

introducing the idea of **proof-of-work,** which was to become a major part of the Bitcoin consensus mechanism.[40] This idea, of introducing cost as a means for solving protocol issues, became the means for introducing scarcity and economic dynamics into protocol designs, and would later give rise to the field of cryptoeconomics.

For those not familiar with the ideas, proof-of-work is one of the more dense and unfamiliar aspects of the Bitcoin architecture. It is also a form of cryptographic proof, again making use of hashing. Nodes in the Bitcoin network are required to do some 'work' in order to be allowed to verify transactions: transactions are witnessed and then grouped into blocks, which they then run through a hashing algorithm.[41] But the output needs to meet certain requirements in order to be valid, namely it has to output a string with a certain amount of zeroes in front, for example 000000000019d6689c085ae165831e934ff763ae46a2a-6c172b3f1b60a8ce26f (the proof-of-work hash for the very first Bitcoin block of verified transactions). In order to produce a valid output, nodes try adding a random number (also referred to as a nonce) to the transaction data. They keep hashing different nonces with the transaction data until the output meets the requirement. This output is then the 'proof-of-work' and is published along with the nonce. Anyone can then check that the 'work' indeed has been done, by running the transaction data and the nonce through the hashing algorithm again to see if it produces the same output. This computational 'work', of repeated hashing of transaction data with different nonces in order to find a valid output, is called **mining** in an explicit reference to gold mining.

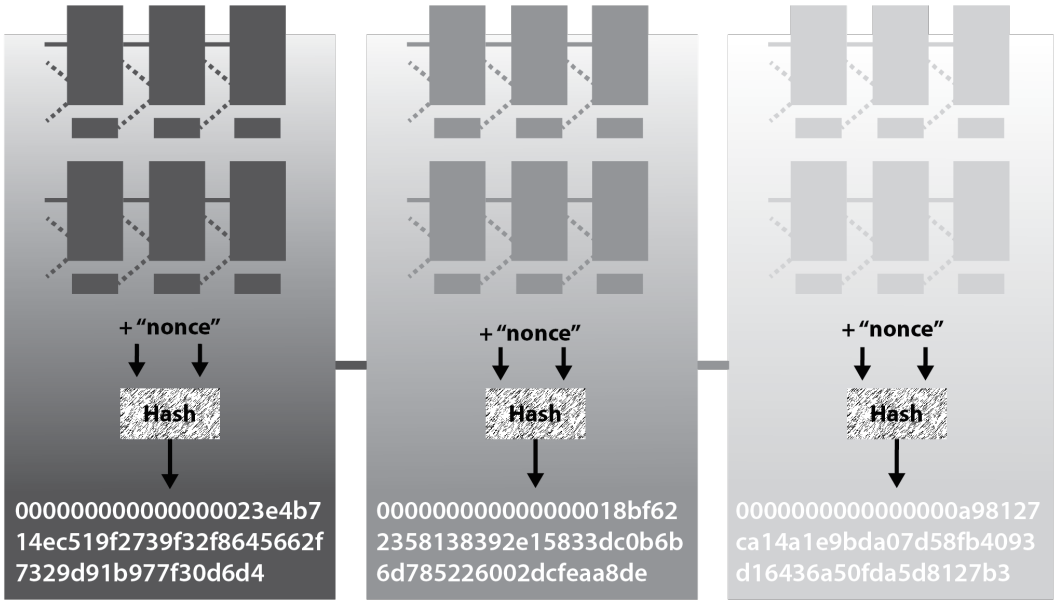

Figure 2. Transactions are grouped into blocks that are hashed with a 'nonce'. The hash output has to meet the requirement of the difficulty target, namely that it begins with a certain number of zeroes.

[40] Since Bitcoin, alternative consensus algorithms using cryptographic proofs in different configurations have been developed and have become an area of research, development and creativity. See proof-of-stake, proof-of-presence, proof-of-cooperation, etc.
[41] The hashing algorithm used in Bitcoin is SHA-256.

The proof-of-work algorithm also operates as a solution to another significant problem for a decentralised payment system, namely how to get the network to agree on which transactions to consider valid, and how to secure the integrity of these records. This is also known as the 'double-spend problem' in Bitcoin, or the 'Byzantine Generals' Problem' in decentralised networks more generally (Lamport, Shostak and Pease, 1982).[42] In a double-spend attack, a person might broadcast a transaction to some recipient to one part of the network and then try and spend that same transaction again by broadcasting a different recipient to another part of the network. In such a case, the decentralised network would require some method for agreeing on which transaction should be considered valid, without resorting to some external authority to settle matters. The competition to find a valid proof-of-work thereby functions as a provably random way for nodes to take turns in verifying transactions, ensuring that no node gets to continuously verify transactions (which would in essence make them an authority). The difficulty of the computational problem is known, and so the solution, what is called the 'proof-of-work', cannot be faked, making each round an open competition for verifying transactions in which it is unlikely for any single actor to repeatedly 'win' and be able to determine transaction verifications at will. In other words, it is intended to guarantee a certain (and measurable) level of randomness in who gets to verify transactions in such a manner that verification cannot be consistently manipulated. Nakamoto compares this to voting:

> Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.
>
> – Nakamoto, 2008, p. 3

The voting analogy is of a peculiar kind (and turned out to be far from equal). Because mining is competitive and a whole network of computers are mining blocks, **consensus** on transactions is an emerging property: a miner elsewhere in the network might mine a contradicting block, which would cause what is called a **fork** in the blockchain. The protocol is therefore set so that the longest chain is the one that is considered valid. As more blocks are mined on a given chain it diminishes the possibility of a different, conflicting fork of the chain being longer and 'winning out'. Mining a block in this sense also signifies agreement with that chain of transactions. It is in a sense a way of 'voting' on a given record of events.

[42] First described in Lamport, Shostak and Pease, 1982, the Byzantine Generals' Problem presents an example of an attack on a city by the Byzantine army: a number of generals have surrounded the city and communicate with each other via messengers in order to coordinate their actions. Knowing that a few of the generals might be traitors passing false messages, the question is how to ensure that the generals reach agreement on a common course of action. This example is used to describe a problem in computing of how to ensure reliability of the system if one component malfunctions (as described by Lamport et. al.) or in a distributed computing network where some nodes might be malicious, provide false data or attack the network.

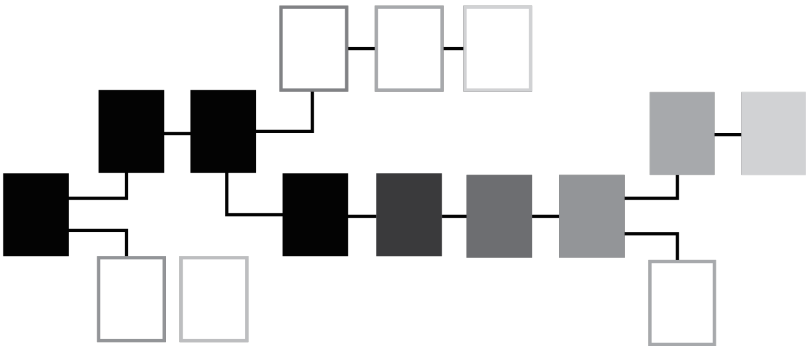

Figure 3. The longest chain in the blockchain is always considered the most valid, represented here by the coloured blocks. Read from left to right, the lighter blocks are more recent and thus less 'confirmed'.

Because the longest chain is the most valid, in order to attack the system, for example to attempt a 'double-spend' or to change the transaction data, one would have to mine blocks faster than the rest of the network. An attacker would therefore in effect have to control more than 50% of the **hashrate** (another way to say mining power) in the network. It is therefore claimed that the security of the network increases as it grows and gains more overall **hashing power** (the amount of computational power that miners are putting into mining blocks) because it becomes more and more unlikely for any single actor to dominate or control all the mining nodes in the network.[43] As the chain gets longer it therefore also becomes increasingly unlikely and it becomes impossible to change the history of transactions.

There is another aspect to the proof-of-work consensus algorithm, which was to instigate an entire new field of computer engineering research. The repeated attempt at finding the nonce is called 'mining', because new bitcoins are created and distributed in the process. The intention with this design is to reward the work done to verify transactions and to do so in a way that would make it more profitable to contribute in this sense than to attempt an attack.

> He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.
>
> – Nakamoto, 2008, p. 4

[43] It is worth noting a private conversation from early 2017 with the head of security for one of Google's subsidiaries and cryptography expert, who mentioned that if the Bitcoin network gained enough value it would be trivial for a company like Google to dominate the hashing-power of the network, essentially breaching the security model. However, the question of what effect that would have on the network is a difficult one as it would rely on the assumed legitimacy of Google amongst the majority of users at that point, as it is likely that the current composition of users would leave the system if such a takeover took place. But the issue his comment points towards is that problems of security and authority might not in fact have been solved by the decentralised architecture but rather still rely on questions of legitimacy amongst ordinary users, as well as questions of network effect and choice in the face of breach of security and legitimacy.

Mining is a competition for verifying transactions in which the incentives to do so are intended to act as deterrent for attackers. This has essentially entailed the introduction of economic dynamics into network security engineering and with it the field of cryptoeconomics, which draws on incentives for decentralised protocol designs. It has since inspired more research in this direction in which the behaviour of economic agents are employed in cryptographic and computational research and the development of security models and new consensus algorithms (cf. Eyal and Sirer, 2013; Bonneau *et al.*, 2015; Kiayias, 2015). The difficulty of the computational problem of finding the right nonce is set so that it is solved on average every ten minutes, thereby simultaneously determining the rate of money creation in the network until a total of 21 million bitcoins are in circulation.[44] This is one of the more explicit references to deflationary and right-wing economic ideas as discussed by Golumbia (2016) and expanded on in Chapter 5.

The cryptographic proofs I have explained above and their relation to the Bitcoin network architecture and economics constitute the technical as well as political proposition of the Bitcoin. They constitute the processes and systems proposed to construct truths about events and certainty of records, in the absence (or intended absence) of any authority or trusted third party that might normally determine such things. Mining and the proof-of-work consensus algorithm form one of the more difficult aspects of the architecture to understand because they so radically re-conceptualise a whole range of problems and processes: *incentives* (mining rewards) are used to motivate *competition* (mining) to *verify transactions* (create a block), which simultaneously *determines the rate of money supply* (the mining rewards are new bitcoin), securing the network by disincentivising attacks and solving the problem of computational consensus (verifying transactions and ensuring integrity of value tokens). This particularly dense set of solutions is also an area of debate and differentiation as it draws in and operationalises concepts from classical liberal economics and game theory through an arrangement of mathematical probability and cryptography, consumes a large amount of energy and has had centralising tendencies.[45] Other cryptocurrencies have in response sought to develop different consensus algorithms drawing from other economic, technical and social theories.[46]

[44] The initial reward was 50BTC per block, which is halved every so often as the network grows, currently at 12.5BTC, with an absolute limit of 21million BTC in the system. After this, the intention is that miners will continue to mine blocks and validate transactions, but will be rewarded through a system of transaction fees instead of new 'coins'.
[45] And indeed much thinking from the Mont Pelerin Society, most notably Friedrich von Hayek, see for example Golumbia, 2016 for a more in-depth tracing of right-wing economic thinking in Bitcoin.
[46] It is also one of the more criticised aspects of Bitcoin as it is considered a waste of energy. Other cryptocurrencies and blockchain projects have developed different consensus protocols for exactly this reason (see comparison of proof-of-work, proof-of-stake, proof-of-cooperation and so on). Proof-of-work remains by far the most used to date. Many of the other consensus algorithms are still being tested and developed.

This complex entanglement has been described as 'truth machine' (Vigna and Casey, 2018) and a 'magic computer' (Buterin, 2015), but it is worthwhile and important to disentangle how 'consensus' or 'truth' is arrived at and what 'magic' is in operation in the blockchain consensus algorithm.[47] If we take a closer look at how double-spending is solved and how consensus is arrived at in a decentralised network, there is in fact no need to determine *which* of the conflicting transactions is true because from the perspective of the system, it does not matter which is verified, as long as it is just one of them. What is 'true' or what 'really happened' is not of importance; these concepts are replaced by randomness and probability in the selection of which node (miner) gets to determine the 'truth' of which transactions happened in this round. Because the work of mining cannot be faked, each round is an open competition for being the node that determines which transactions are valid and thereby considered true in the network. The 'consensus' of the consensus algorithm should therefore not be misunderstood as some sort of agreement on the truth of events but rather as an incentive-driven settlement, the truth of which is decided on through randomised turns determined by expending CPU power. The 'fairness' of the consensus algorithm, or, rather, its legitimacy lies not in negotiations, consensus of opinions or some notion of justice or objective truth but in randomness and large numbers generating an operational computational consensus for the network.

I have described the Bitcoin protocol and consensus mechanism as well as the ways in which cryptographic proofs, along with a decentralised architecture and economic incentives, are assembled with the aim of resolving the need for and possibility of authority. These descriptions and systems designs have an effect in their own right that exceeds their technical efficacy. They are convincing and powerful means of spreading and circulating ideas. This is acknowledged by several other authors who address a distinction between what is promised by the technology and its actual effects (Golumbia, 2016; Reijers and Coeckelbergh, 2016). But where Golumbia, for example, understands the Bitcoin architecture and its descriptions as vehicles for an economic ideology, I argue that the Bitcoin whitepaper and its systems architecture is convincing and powerful as a promise of an apparatus that is external to and beyond the control of human beings to replace authorities. In a sense, it is so convincing as to become more real to some than the ways in which the system affects people and contexts in which it is used, what I have called a 'systems primacy' (Nakamoto, Bridle and Brekke, 2019) whereby the deterministic capacities of cryptography become a certainty upon which all else can be constructed. This apparatus does indeed draw on markets as one element of arranging some exterior that would be more objective than humans, but as one ingredient of several. The deterministic conditions that are arranged in the architecture, verified and secured through cryptographic proofs, rather promise to finally resolve age-old

[47] See https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/

issues of authority by replacing it with a provably secure, decentralised and therefore fair system. It suggests a promise of an objective, mathematical resolution to subjective, corruptible humans.

4.1.2 Determinacy – trustless perfection and mushy humans

> Bitcoin is this perfect/trustless/mathematical machine, built – most unfortunately - upon a foundation of mushy humans.
>
> – Gareth Williams, Bitcoin developers' email list, April 27th 2014[48]

Cryptographic proofs promise the ability to determine trust. These are mathematical proof of events, relationships, ownership and decisions, indisputable because they are founded on mathematical rather than human statements. These proofs are understood to solve the problem of trust because they state what can be known, the construction of a scientifically provable fact, which in turn can be used to create deterministic systems and architectures. The Bitcoin whitepaper for many therefore described a 'perfect/trustless/mathematical machine', where the only flaws came about because it was necessarily built upon 'a foundation of mushy' and imperfect humans (see quote above). There are a few problems that come up when such mathematically proven, deterministic architectures go from being a specific strategy for certain purposes, in relation to specific authorities, to a general proposition to resolve the issue of 'authority' altogether. As a general proposition, the problem becomes how to understand and make sense of the limits of this form of determinacy. For example, the system itself is conceived, developed, maintained, used and built by humans, with and alongside specific material, social and economic contexts, which cannot be fully determined and secured through cryptography alone. A person can steal someone's cryptographic keys and their funds, or cheat them on a cryptocurrency exchange; these situations matter a whole lot to those who experience them, but the transactions would nevertheless enter into a blockchain and be cryptographically proven and secured simply as transactions that have taken place. This raises the question of where exactly the limit to cryptographic proofs resides and what type of 'trustlessness' they construct, as well as what they can do in the mediation and enforcement of relationships, trust and truths and the system's ability to determine things.

The science and engineering of cryptographic proofs do 'work', in the sense that they are able to prove, secure and determine events and relationships, and yet it is clear that there is a limit to what these can determine and for whom. To put it differently, the Bitcoin architecture is trustless up to a certain threshold, and yet for most people, it actually requires a lot of trust in

[48] See https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-April/005615.html

order to use. The user has to 'trust' in the cryptocurrency exchange where they might purchase bitcoin, their listed exchange rate, the wallet developer, an online explainer of how cryptographic keys work and so on. How then to reconcile the science, the mathematics that makes up the trustless solution of Bitcoin, and the experience of using it? In the Bitcoin whitepaper, the problem with existing payment systems and the intermediation and authority that these require is articulated as one of trust. The problem that Nakamoto articulates is that trust requires mediation in cases when trust breaks down, and mediation is an extra cost and potential security threat. Developer Maxwell expands on this on the Bitcoin developers' mailing list, a quote that is reminiscent of many other such descriptions of the radical potential of Bitcoin to resolve the issue of trust and authority:

> Bitcoin seeks to address the root problem with conventional currency: all the trust that's required to make it work—
> — Not that justified trust is a bad thing, but trust makes systems brittle, opaque, and costly to operate. Trust failures result in systemic collapses, trust curation creates inequality and monopoly lock-in, and naturally arising trust choke-points can be abused to deny access to due process. Through the use of cryptographic proof and decentralised networks Bitcoin minimises and replaces these trust costs.
>
> – Gregory Maxwell, Bitcoin developer, 2015[49]

The way that trust is articulated in Bitcoin is as a potential systemic risk and an unnecessary cost. A trustless system, on the other hand, implies that one does not have to trust any aspect of the system, or more precisely, in the good intentions of any other node in the network, as long as the majority of them are honest, in order to know that the network is secure and functions as intended. This became an enticing prospect when expanded from the realm of computer networks to financial, political and legal institutions. Indeed, this formula, in which trust and mediation are understood as problems that can be solved by replacing trusted relations with a trustless system, turned, through Bitcoin and through being generalised in Ethereum, into a vocabulary in the blockchain industry more generally to explain pretty much any problem with existing institutions and systems, and to pose blockchain as a solution to these by solving the 'trust' problem.

The following is an example where this exact limit of trust and trustlessness is negotiated in a discussion on the Bitcoin developers' mailing list from 2011. The discussion itself is not out of the ordinary. It is typical of many such discussions where a person writes to the developers' email list suggesting a patch or improvement to the protocol, and the proposal is then discussed amongst the developers for its benefits or potential security issues. In this email

[49] https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-December/011865.html

thread, a developer who is not part of the core development team, Parkins, raises a possible issue of a double-spending attack: two people in different locations might purchase an item with the same bitcoin, so that part of the network would register one transaction and another the other transaction.[50] It takes some time for the transactions to propagate through the network, and yet more time for there to be enough confirmations (blocks mined) to know for sure which transaction is verified in the blockchain. In the meantime, in his example, at the location of the actual purchases, the scammers might have already left with their goods, leaving one of the merchants with an invalid transaction. The solution that Parkins wants to propose is that if a node detects double-spending it will not only drop the contending transaction, but will also send out a message to other nodes about this already at the stage of propagation before blocks have started to be mined, so that merchants might know immediately if there is a potential issue with their transaction. Bitcoin developer Matt Corallo responds: 'There really is no reason to add the extra network complexity for this.'[51] Corallo's concern is that 'adding more crap to the protocol' could open up other possible issues like DDoS attacks, whereby the network could be flooded by additional messages.[52] For Corallo, the problem of double-spending is already solved in the protocol as is, and therefore doesn't need to be addressed further. For the merchants who might not see the double-spending attempt in time, Corallo suggests a 'Bitcoin backbone' of well-connected nodes that would witness large amounts of transactions and know whether there are any contradicting ones in the network. Parkins, increasingly frustrated, responds:

> *>So, you peer with the largest > miners (a 'Bitcoin backbone' or large miners and merchants has been > suggested over and over again and really hasn't happened) and modify*
>
> It hasn't happened, and yet it seems to be that this non-existent thing is your solution to the problem.
>
> *>your client to, instead of dropping transactions which are > double-spends, keep both in memory pool and consider them both invalid > until one of them confirms.*
>
> Well that's what happens now. But that doesn't help the poor sap who's just handed over some goods. I want it so that small businesses can use the client to give them practical answers instead of this '0/unconfirmed' stuff which requires understanding of the system.
>
> *>This will work with 1, 2, or n scammers, doesn't require any additional > network messages, and offers just as good, if not better security over a > double-spend message.*
>
> I'm not really trying to prevent double-spends – bitcoin *already prevents double-spends. Also: the only difference between your suggestion (don't drop) and my suggestion (don't*

[50] See https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2011-August/000287.html
[51] See https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2011-August/000290.html
[52] See https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2011-August/000296.html

> *drop but mark with MSG*DOUBLESPEND) is a single number in the inv. I really don't get the objection.
>
> – Parkins in discussion with Corallo, Bitcoin developers mailing list, August 4th 2011[53]

What is interesting about this discussion is that although the problem of double-spending is solved in terms of the Bitcoin blockchain security model, the risk still exists in practical terms for merchants. What I would like to highlight here is not the technical trade-off, nor whether Corallo or Parkins are right, but rather that there is a negotiation and separation out of what is a problem in the first place; what should be taken care of by the protocol and what constitutes a risk for and responsibility of those who choose to use the system.[54] What starts to emerge is that there is a gradation of concerns from a systems design perspective, in which what is understood as an attack and security issue relates firstly to whether it is a threat to the survival of the system itself. For Corallo, if merchants care about the time it takes for sufficient confirmations to avoid double-spending they should make sure they are 'peered with a well connected node'.[55] It is an explicit decision about what is the responsibility of the protocol design and what is the responsibility of those choosing to use it. My argument is that this also defines the exact limit of the proposition of trustlessness and disintermediation. The merchants would trust a large miner supernode in order to run their businesses. For them, Bitcoin would then no longer, strictly speaking, be trustless. There is therefore a limit to how the Bitcoin architecture resolves the need for trust and determines and secures relationships. While this might seem obvious in the sense that a given technology cannot account for any and all of its potential uses and effects, this limit poses a philosophical problem to the fundamental claims of resolving authority as a general proposition. It raises the question of for whom or for what purposes exactly it 'resolves authority'. For the hypothetical merchant in question, a 'Bitcoin backbone' of large miners would simply become another new form of authority, and this new authority has as of yet very few accountability measures and an operational merit that is both unfamiliar and as of yet undefined.

This question, of who a given systems design serves, is addressed in different ways in Bitcoin and various other blockchain projects, and many engineers and developers are very concerned about the risks and issues faced by different users of the systems. But the promise of a mathematical resolution to authority more generally has also given rise to a tendency in Bitcoin and blockchain to what I call a 'systems primacy'. In these accounts, a problem faced by a merchant, such as the one described above, or any of the other scams and scandals that have happened in Bitcoin would be assigned and explained as a problem of imperfect

[53] See https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2011-August/000291.html
[54] Although Corallo does seem to have a point, that if the given node is slow to receive a potentially conflicting transaction message, there is no reason to believe that an extra kind of message about double-spending will do much other than multiply the amount of messages in the network.
[55] See https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2011-August/000296.html

humans. As in the quote at the beginning of this section: 'Bitcoin is this perfect/trustless/mathematical machine, built – most unfortunately – upon a foundation of mushy humans.'[56] Describing the system as perfect and humans as mushy serves a purpose. It entails a cut, determining what matters and what is excluded from mattering in the claims made of Bitcoin. In the meantime, a Bitcoin protocol is not the only sensibility to enact this cut, and is not the only determinate agency in the deployment of the system.

In Baradian terms, the Bitcoin protocol can be understood as an apparatus that entails a certain onto-epistemological sensibility with determinate effects. Above I have described some of the more specific ways that this sensibility comes to matter in whitepapers, protocols and so on (which begins to open up how what matters cannot be fully determined through a single sensibility, evident across further materialisation in hardware and so on). As a Baradian apparatus, however, the 'objectivity' of the apparatus is not due to it being external to necessarily subjective humans. Instead, objectivity entails the ability to accurately describe the conditions to reproduce a certain determinate assemblage. The human, knowledge, papers and whitepapers, mathematical and market models, hardware and so on are part of what makes things matter. Because of this, there is a limit to particular modes of determinacy. Not everything is or can be determined through the protocol and the protocol is not the only determining agency. The trustless conditions that are sought to be determined have a limit and that limit also signifies exactly what specifically is being solved by determining certain relations and for who/what.

The deterministic conditions promised in the model are, from a 'systems primacy' sensibility, all that matters. Anything else is rendered *insensible*; they should not and cannot be sensed as mattering because there is no mathematical proof. This is entirely coherent with the idealized description and sensibility of Bitcoin. This drawing of a boundary between a coherent and perfect core and mushy, imperfect humans allows for the integrity of the idealised system to remain intact while, for all practical purposes, trusted intermediaries proliferate (necessarily, as we have seen for the use of the system), the code is continuously updated and maintained (by mushy humans) and hacks take place with money lost. Such articulations are quite common in discussions on Bitcoin, blockchain and cryptocurrencies, but affinity with the 'perfect machine' does not always take such explicitly ideological forms. At other times, instead of 'mushy humans' this might be construed as an interaction between the perfect system and a 'clueless end-user'. In these cases too the system itself is considered secure and coherent, and DDoS, and what are called Sybil and Finney attacks might have been addressed, whereas hacks and the collapse of exchanges, for example, are considered issues to do with user concerns rather than the Bitcoin blockchain itself.

[56] See https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-April/005615.html

The solution here is not necessarily to include what has been rendered insensible into the Bitcoin sensibility. It is not necessarily that Corallo should take Parkin's concerns into consideration and solve all the problems of merchants through the actual protocol itself. What I am highlighting is that this very limit to the trustless deterministic promises of Bitcoin matters, because it shows precisely the limits of what is taken care of in the protocol, and for whom, and what might need to be taken care of through some other arrangement. What this entails is to become aware of other sensibilities that the system and protocol might touch upon, and that much of the political effect and meaning of Bitcoin takes place here. Indeed, in the years 2016 and 2017, the deterministic claims of both Bitcoin and Ethereum as resolving issues of authority faced major crises. This shook many of the deterministic understandings, which began to loosen into more sophisticated ways of addressing power, trust, humans and authority (see Chapter 6). An interesting contradiction in deterministic understandings of Bitcoin as an objective system beyond the control of humans is that such claims require that such a system be simultaneously determined solely through a human agency – the author(s) of the Bitcoin whitepaper Satoshi Nakamoto – as well as entirely removed from human control. It assumes complete control in establishing a determinate apparatus that would be beyond all control. In part, I would argue, this contradiction is accommodated for through the disappearance and continued anonymity of Nakamoto. This disappearance also signified a disappearance of authority, which is necessary in order for the system to be beyond control, while allowing for the possibility of an initial inception of complete knowledge and control. Issues with the system design can then be argued as the problem of necessarily and unfortunately mushy humans, not pertaining to the original vision. What this also means is that highlighting the discrepancies between the stated deterministic vision and its implementation is not sufficient for challenging a deterministic understanding of Bitcoin because it merely points to issues requiring correction. A protocological analysis, whether as a critique (Bitcoin does not 'work') or intended as simply an explanation (this is how Bitcoin 'works') is not sufficient in other words, because it takes as a starting point that the only thing that matters is the protocol. It takes the acknowledgment of other sensibilities and determining agencies to allow other things to matter.

4.1.3 Emergence – a node is not just a node

In his book from 2004, media theorist Alexander Galloway analyses the internet, looking to understand how control happens in decentralised systems (Galloway, 2004). He articulates a form of protocological power that operates by shaping the landscape of possible and desirable behaviour: in contrast to a 'disciplinary power', with stated regulation that punishes after the fact, 'protocological power' operates in an immanent manner, an immediately executing law, written in an executable language, that operates continuously by shaping the landscape of desirable action. This analysis is interesting in relation to Bitcoin and blockchain

in that it describes so perfectly the ambitions and intentions of such systems, namely to eliminate disciplinary power and replace it with what is considered a more neutral, protocological power that does not operate through violence and punishment, but instead through incentives and immediately executing code.

In this light then, it should be possible to reveal 'the politics' and political implications of Bitcoin by analysing its protocol. Indeed, the description and analysis of the Bitcoin protocol and systems design that I have engaged in above illuminates some of the ways in which particular sensibilities are materialised and sought to be encoded into the protocol, and this to some extent then does 'tell' something of the politics of Bitcoin. Through a protocological analysis I am able to describe the potential for cryptographic proofs to mediate trustless situations, the system itself becoming a trusted intermediary on the basis of mathematically-determined high improbability of anyone being able to cheat, given the known deterministic conditions. Through this careful description I am also able to point to the exact limits of claims of trustlesness and determinacy – a concern that is rarely addressed explicitly but that is fundamental for practical applications of Bitcoin (and blockchain more generally) to make sense. The whitepaper, whether 'true' in its implementation or not, has a political effect in and of itself by presenting a particular project and justification of how Bitcoin intended to work. However, protocols do not fully and finally determine outcome in terms of effects. This is one of the pitfalls of a protocological analysis; to assume that a design, whether understood as determined by human assumptions or intent, or transcendental mathematical laws, deterministically produce some form of effects.

An analytical approach that looks to explain the full implications of a system by analysing the protocol alone would merely replicate assumptions that everything can be explained through the protocol, that its implications are fully determined here. It assumes, in a sense, too much control and determinacy. In the meantime it also construes the political stakes in terms of whether a 'good' or 'bad' ethics or politics is encoded (it makes the project one of behavioural and total engineering). In the following, I carefully trace through the limitations to such an approach through the question of centralisation of Bitcoin mining, with the intention to arrive at an analytical standpoint that does not rely entirely on protocological determination, but takes into account mushy humans and multiple sensibilities of what matters and how things come to matter and allows space for the insensible.

In the Bitcoin whitepaper, nodes are described more or less as equal. Here, the whitepaper outlines what nodes in the Bitcoin network do, and the process of how transactions would take place:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

– Nakamoto 2008, p. 3

The whitepaper describes a network where transactions are broadcast to *all nodes*, that *each node* collects new transactions into a block and so on, a network of equal nodes performing work for each other. The description is reminiscent of typical diagrams illustrating 'decentralisation', dots connected to other dots via lines, nodes communicating with other nodes of equal sizes in what looks like a harmonious and horizontal arrangement. It looks democratic, everyone is participating and it gives an intuitional sense of equality. Networks as they are built and operate are more complex than that; they might be designed to communicate with nodes according to all kinds of criteria, including closest, farthest, most capacity, best reputation or otherwise. They also change over time and have important emergent characteristics. The Bitcoin network is indeed 'open' and anyone can theoretically contribute and set of up a node by downloading and running the Bitcoin client, but in the years since the Bitcoin whitepaper was published and the first Bitcoin transaction was registered, these tasks have become increasingly more specialised.[57] Not all nodes necessarily '[collect] new transactions into a block'; Bitcoin wallets that will simply broadcast and witness have been developed and are widely used. Many of these wallets present an interface and do not necessarily give people control over their cryptographic keys, implying several layers of 'trust' for those using these services. From the intention of trustlessness this might be considered an undesirable compromise, but for someone not used to handling cryptographic keys, and generally not concerned with this notion of trust, it might be a more usable system, as long as there are other available accountability structures for the given wallet.

Furthermore, not all nodes 'work on finding a difficult proof-of-work for [their] block[s]'; full nodes that might broadcast and witness transactions and check that these comply with the consensus rules, but not mine blocks, have emerged. This has largely been in response to

[57] See https://github.com/bitcoin/bitcoin

mining becoming so competitive and difficult that so-called mining pools have developed.[58] These pools look more like a federated system than a decentralised system. In the Bitcoin whitepaper, the ability to mine is described as determined through CPU power. But as competition to mine increased, new, dedicated hardware was developed, so-called Application Specific Integrated Circuits (ASICs), replacing CPU and making mining increasingly specialised and difficult to take part in. The development of ASICs is understood to have contributed to the centralisation of mining, and from this larger concerns over miner's control of the Bitcoin network have emerged. In addition to nodes specialising, an entirely new network layer called lightning network, has been developed to allow faster transactions in parallel with the Bitcoin main net.[59] In other words, a node is not just a node, and a network is not just a network. These develop and emerge into new specialised roles and configurations, and do so in relation and response to conditions such as mining incentives, hardware development, exchange rates, geographical location and conditions, legislation and so on. The Bitcoin network has emergent characteristics and also contingent effects that challenge any simple description of the system as 'decentralised', 'disintermediating' and 'trustless'.

These emergent effects, such as the centralising tendencies of Bitcoin mining, could be, and are, critiqued for their discrepancy with the original vision, used as an argument for how Bitcoin does not 'work' – that it claims to be 'decentralised', but in fact centralises. The problem with such an approach is that it argues from a deterministic standpoint: it presupposes that the protocol *would* be able to determine a decentralised system but that it doesn't and that therein lies its faults. In fact, any analysis that overly relies on the claims of the protocol would come up against this issue of merely replicating a deterministic assumption of what protocols are able to do. In the meantime, engineers, enthusiasts, and so on are aware of the centralising tendencies and actively look to correct these as part of an ongoing effort to materialise what matters to them. The centralising tendencies of, in particular, Bitcoin mining form a well-known issue that subsequent cryptocurrencies and blockchain protocols have sought to address in new consensus mechanisms as well as hardware designs, for example countering the development of ASICs or basing consensus on stakes or other criteria rather than a hashing competition.

The technical literature on blockchain is a rapidly expanding dynamic field, and while it is concerned with improving technical aspects, it would be a mistake to take these efforts as an uncritical engagement with how the technology develops. Critiques of technologically determinate claims made of blockchain risk reinforcing deterministic understandings of protocols if based on an ontological division between the social and the technical, because

[58] See for example https://www.antpool.com/ and https://pool.bitcoin.com/

[59] See https://lightning.network/

the issue then is construed as a conflict between who is the most appropriate agent of control and determination, the human or the machinic. This also makes for disciplinary divisions where social sciences take care of, and are necessarily on the side of, 'the social' and human, while computer sciences and engineering address 'purely technical' questions. The technical literature on blockchain projects in many ways distinguishes itself as explicitly and self-consciously political, having largely emerged as an intervention into the political economic order (Meiklejohn *et al.*, 2013; Musiani *et al.*, 2016; Sirer, 2016; Azouvi, Maller and Meiklejohn, 2018; Buterin, Hitzig and Weyl, 2018). And so many of the social, political and environmental issues critiqued from the 'outside' are or tend to become areas of concern in the design and engineering, and are addressed in the form of new technical problem spaces. A critique of Bitcoin based on its failure to live up to its claims does nothing to challenge the idea of a system based on cryptographic proofs beyond control. It merely points towards a discrepancy in its implementation and thereby describes some aspect of the world that needs to be reorganised, corrected or reconfigured to materialise the vision.

Rather than looking to access 'the technical', opening up the protocol, in order to critique its politics (with an aim to changing it 'for the good'), an awareness of the insensible suggests a different approach that instead points to the limits of determinacy and how those limits are worked with. There are theorists in social sciences that are beginning to question the analytical strategy of 'opening the black box' in order to understand the ethical, political and social consequences of, in particular, digital networked technologies. Burrell discusses 'opacity' in relation to machine learning (Burrell, 2015), in the sense of 'corporate or state secrecy' (pp. 3-4), and 'technical illiteracy' (p. 4), but also, and importantly in terms of the scale needed for useful application, that machine learning requires large amounts of data, and indeed makes sense of this data in ways that are not fully understandable for human scale reasoning and styles of semantic interpretation (pp. 4-5). Amoore also challenges the idea of gaining full transparency of datascapes that are emergent and ever-changing (Amoore, 2016), focusing on the ways in which technologies used for targeting and profiling work *with* the unknown, operating on probabilities and risk in constantly changing conditions rather than seeking complete oversight and certainty (Amoore, 2013, 2014). Seaver discusses the problem of 'knowing algorithms', given that their deployment, behaviour and effects are highly contingent and contextual, changing depending on the changing profile of a given user, for example (Seaver, 2014). Each of these question the idea that there is a single privileged vantage point that might reveal the full implications of an algorithm, protocol or system. Instead, everything potentially matters, and what matters more concretely depends on what or who is of interest, on where the cut is drawn. While there are important differences between systems deploying algorithms that are explicitly contingent on and operate through changing data, and the Bitcoin core client protocol and algorithms, which are deterministic, these insights are helpful for addressing the problem of assuming complete insight revealed

through a protocological analysis. Where Seaver and Amoore point to the ways in which the implications of algorithms are largely determined through and change along the data that they interact with, in ways that are less concerned with predicting known futures and more with opening up potentials (see also Amoore, 2013; Amoore and Raley, 2017), the Bitcoin protocol and its effects as a network system are also emergent in that they interact with and are deployed across differing and ever-changing contexts. Describing and analysing only a Bitcoin sensibility and its particular form of determinacy is to ignore the significance of its effects in, amongst and in relation to that which has not been determined, or is indeed determined by other sensibilities. This occurs in two distinct ways, namely the insensible that was not sensed as mattering from the perspective of those designing cryptographic systems, and the insensible ways in which a given system might matter. A political analysis focusing solely on a Bitcoin sensibility and materiality in and of itself is not enough, then. But also, and importantly, to exclaim that something has been excluded, such as the centralising tendencies of mining, is not enough either. It would merely suggest taking into account that which has been excluded, which in turn is to render it sensible to a deterministic protocological sensibility. A critique of a Bitcoin sensibility on the basis of it failing to successfully determine a given context or condition provokes either an expansion of the sensibility to include and reconfigure this missing element, or its productive *exclusion* from the realm of what matters; it is pushed into the realm of 'mushy humans'. Instead of a description and subsequent assessment of a Bitcoin sensibility on such terms, then, my aim is to articulate a philosophical position in relation to the Bitcoin protocol that resolves the question of limits to the deterministic relations of cryptography by instead acknowledging the insensible, that which has not yet entered into a given sensibility – and possibly never will. This creates a space for cryptographic proofs to actually be considered to 'work' within certain contexts, but also to direct awareness to the limits of this mode of determinacy such that it becomes necessary to state whom and for what it 'works' and how it relates to other sensibilities.

4.2 Algorithmic animism

> One of the best descriptions of Web3: Consider Web 3.0 to be an executable Magna Carta - the foundation of the freedom of the individual against the arbitrary authority of the despot. @**juanbenet** quoting @**gavofyork** at #**web3summit**. Couldn't agree more.
>
> – Jutta Steiner CEO of Parity, Tweet from the 2018 Web3 Summit[60]

[60] See https://twitter.com/jutta_steiner/status/1054336890718031874

In late 2013, a new project called Ethereum was proposed; this was to become the second largest cryptocurrency network and one of the first to articulate 'blockchain' as a protocol level innovation independently of and exceeding application-specific uses as a transaction system. Ethereum was launched as a project to generalise the Bitcoin blockchain and make it Turing-complete. Instead of only witnessing, verifying and registering transaction messages, the particular arrangement of cryptographic proofs, decentralised networks and economic incentives that had been invented with Bitcoin would be reconfigured to witness any kind of data, including code, as well as incentivise its execution in a decentralised network. The idea was no less than to transform the way the internet operates, suggesting a 'Web 3.0', realising an ambition that many technologists of the internet have been concerned with, namely to 'redecentralise' the internet such that it would not longer be dominated and run by a select few companies, but instead would be facilitated and run by a network of peers. Addressing the protocol layer, this arrangement would be an 'executable Magna Carta' as suggested by Ethereum co-founder Wood (quoted above in a tweet by Steiner, founder of Ethereum company Parity, and ex security chief of the platform) and would be so in the sense that it would define a networked space that would operate on rules that were immediately executed, because these would be written in code, an executable language. Such a network would thereby be secured from 'the arbitrary authority of the despot' because it would be realised through a decentralised architecture and secured through cryptography. Code, decentralisation, cryptographic proofs and economic incentives would form and secure a network space that would be beyond the control of authorities. Authority in the meantime had taken on a broader meaning, derived from network security models, to include any potential aspect of the system that implied trust, and would therefore rely on a potentially corrupt/ible human. The project became a promise of a protocol layer with applications that would be beyond the control of any human, including the founders themselves. Such an apparatus promised an 'incorruptibility of judgement, often difficult to find' that 'comes naturally from a disinterested algorithmic interpreter' [sic] (Wood, 2014a, p. 1). This laid the groundwork for a determining agency beyond the control of humans, that I approach and discuss here as an algorithmic animism. I do so not to point towards some form of computational superstition but in order to work through how that which is beyond control is made sense of, more specifically in the ways that the concept of autonomy is reconfigured in and through suggested Ethereum applications.

This section and the second half of this chapter are structured as follows: I first describe the Ethereum architecture and the ways in which it generalises concepts in Bitcoin to make them operational in a platform intended to run any kind of application, currency or protocol.[61] I focus in particular on how economic concepts are operationalised for computational purposes,

[61] Indeed, the Ethereum platform not only signified the generalisation of blockchain but also a move to *platformise* protocol development, discussed further in chapter 5.

drawing economic dynamics deep into the security model and operations of the platform. I then discuss how the understanding of trust and trustlessness in the security model of decentralised networks lays the ground for specific understandings of autonomy and control, shifting these to the non-human and non-human modes of determination, which I discuss in relation to two main applications envisioned for Ethereum, namely *Smart Contracts* and *Decentralised Autonomous Organisations* (DAO). The conjuring of agencies beyond human control provoke responses that might reclaim and reassert human control and therefore also responsibility. Instead, in the final section, I look to animist readings to sidestep the need for control as a basis of responsibility (and with it, ethics and politics). Such animism can and does to some degree amongst the Ethereum community suggest the necessity of a non-human agency operating at scale and along a mathematical logic beyond human reasoning. I draw on the idea of the insensible and Barad's multiple forms of determinacy and the indeterminate as a means to counter the necessary expansion of an algorithmic determining agency, without reverting to assumptions of the possibility of full knowledge and complete control by humans.

4.2.1 The Ethereum architecture

> Ethereum is a project, which attempts to build the generalised technology; technology on which all transaction-based state machine concepts may be built.
>
> – Wood, 2014a, p. 1

In this short quote from an early Ethereum technical paper, developer and co-founder Wood articulates the computing paradigm that the project seeks to realise; namely, to operationalise transactions as a means to change the 'state' in a decentralised network. Much how mining rewards in Bitcoin pays miners to change the state of the records of transactions in the network, in Ethereum transactions would fuel a state change expressing any kind of 'machine concept' (Wood, 2014a). I will explain this in more detail below, but first, in order to get an overview, the following table shows some of the main technical differences between Bitcoin and Ethereum and the ways in which Ethereum seeks to expand on and generalise the Bitcoin system. (The table compares general differences in the architectures of the Bitcoin and Ethereum based on their whitepapers).

Bitcoin		Ethereum	
Bitcoin	A cryptocurrency used as speculative asset, store of value, payment token and reward for mining and payment of transaction fees.	Ether	A cryptocurrency used as speculative asset, store of value and payment token.
		Gas	Ether is referred to as '**gas'** when used internally in the Ethereum Virtual Machine to pay the **gas price** of executing a given computation.
Account (address)	An account has an address that is associated with a number of bitcoin on the blockchain. The account is accessed and controlled by a human using a cryptographic **keypair**.	External account	Has an address and a 'nonce' and are similar to Bitcoin accounts in that they are controlled by a person with a cryptographic keypair and can hold an amount of Ether.
		Contract account	Has an address, a 'nonce', contract code and stores data used by the contract. It's held on the blockchain (across all full nodes) and can be changed by paying the **gas price** to execute the code. Once written, it is controlled by its contract code and executes when prompted to by anyone in the network.
Transaction	A person can send bitcoin to another person's bitcoin address by accessing their account using a **private key** and signing a hash with the next owner's public key.	Transaction	Similar to bitcoin transactions, a person can send ether to another person's account.
		Message	Accounts can send 'call' messages to contract accounts to execute code.
Mining	Verifies transactions and determines money supply through the rewards paid to miners.	Mining	Verifies and executes transactions and contract code and determines money supply.
Blocks	Contain verified transactions.	Blocks	Contain verified transactions, as well as the 'state' of the Ethereum Virtual Machine, meaning any changes to contracts and new ones that have been created.
Transaction fees	Transactions include fees paid to miners for verifying them. When the total amounts of bitcoin (21mil) are created, this will ensure continued 'incentives' for miners.	Gas price	A gas price must be included for each computational step required in order to execute a contract or transaction and is paid to miners for running the code.
Rewards	Miners receive a reward of a number of newly create bitcoin when they successfully mine a block. The mining reward started at btc50 per block and is halved every so often until a final cap of 21 million bitcoin is in circulation.	Rewards	Miners receive a reward of eth3 of newly created ether (as of writing), and 0.625-2.625 for miners who successfully mined but whose blocks were not included in the consensus chain. A cap on ether supply is set at 18 million new ether per year.

Table 3: comparison of Bitcoin and Ethereum architectures.

In Ethereum, the blockchain is used not only to manage transactions of the cryptocurrency 'ether' but also for storing data and code for applications and contracts that are run across the network of full nodes. These two purposes correspond with two different forms of accounts; the first called **external accounts** that are similar to Bitcoin accounts and controlled through

a set of cryptographic keys managed directly by a human owner; and the second, **contract accounts,** that comprise contract code, which, once written and deployed on the blockchain operates independently and is run when prompted to, either by other contract accounts or other people's external accounts. External accounts can make ether **transactions** with each other or send **messages** to contract accounts to run code. Contract accounts can also send messages to other contract accounts to run other bits of code independently of external accounts, meaning independently of a human-controlled account, by, for example, releasing funds when some criteria are met. Contract accounts have several elements not included in accounts as conceived in Bitcoin, most notably the contract code and storage that holds any data related to the contract. The code held in contract accounts is referred to as Smart Contracts and are considered 'self-executing' as they are stored in a network beyond the control of any individual, and run when prompted to by any external account or even a different, non-human controlled contract account. Contract accounts 'live' on the blockchain – i.e. across the network of full nodes. Any activation of the contract code that requires a change in a contract's stored data entails what is called 'state transition', executed by miners mining a block and verified by all full nodes. This means that all Smart Contracts and bits of code are witnessed and run by all nodes in the network, making for a very inefficient computer. This is a brief overview of Ethereum. Below I go into more detail exploring how transactions are used to execute code; how this large decentralised computer, although hugely inefficient in terms of speed and resources, addresses 'trust' and therefore suggests an unusual set of possible uses.

Transaction-based computation

In a paper outlining the Ethereum technical architecture, co-founder Gavin Wood re-describes Bitcoin as a 'transaction-based state machine' (Wood, 2014a). The idea was that instead of tracking the exchange of value tokens, the blockchain could be conceived as representing the 'state' of the network, and proof-of-work would be the algorithm that determines changes to that state; a subtle shift in perspective that foregrounds the blockchain, as representing the **global state** of any data in the network, while reconceiving transactions as the instrument for governing changes to the global state. The shift in attention from Bitcoin to the blockchain that was taking place more broadly at the time was met with scepticism in parts of the Bitcoin community, in part because side-lining Bitcoin in this way was seen as a move to make cryptocurrencies less threatening to regulators and financial institutions, but also because for those with an intimate understanding of the role of mining for securing the blockchain, there simply was no 'blockchain' without Bitcoin. The currency was an integral part of the consensus and security model. This was not lost on the Ethereum team, and the currency aspect continues to play a central role in its architecture, as reflected explicitly in a statement by the inventor of Ethereum Vitalik Buterin in an early presentation: *'in order to have a*

decentralised data-base, you need to have security, and in order to have security you need to have incentives, and you need to have a currency.[62] Value tokens were considered integral to the operation of the network because they would be an incentive to run it, keep it secure and contribute to its upkeep. This is a significant difference and change to previous generations of decentralised technologies, and rests on the idea of currency and value tokens as universal incentives. As it turned out, value tokens would not only incentivise security but also attacks on the network.

Ethereum aims at being a 'generalised technology' (Wood, 2014a), but it is a generalisation founded on a set of very specific ideas from Bitcoin. In Ethereum, price mechanisms and monetary incentives are intended to help governing behaviour towards activities beneficial for the system, while preventing attacks by making these very expensive, an expansion of the idea of Bitcoin mining in which miners receive new coins and/or collect transaction fees once they have mined a block. This incentive-based form of network governance is similar to Bitcoin, however the architecture of Ethereum deepens and expands this model of incentive-based network consensus. Protocol design began to incorporate ideas from game theory to psychology and economics to help design protocols that would enable certain behaviours while making others undesirable or impossible – an ongoing modelling of how people might 'game the system' and how that might be prevented.

The step-by-step process of a transaction, as defined in the Ethereum whitepaper, looks like this:

1. Check if the transaction is well-formed (i.e. has the right number of values), the signature is valid, and the nonce matches the nonce in the sender's account. If not, return an error.

2. Calculate the transaction fee as STARTGAS * GASPRICE, and determine the sending address from the signature. Subtract the fee from the sender's account balance and increment the sender's nonce. If there is not enough balance to spend, return an error.

3. Initialise GAS = STARTGAS, and take off a certain quantity of gas per byte to pay for the bytes in the transaction.

4. Transfer the transaction value from the sender's account to the receiving account. If the receiving account does not yet exist, create it. If the receiving account is a contract, run the contract's code either to completion or until the execution runs out of gas.

[62] Vitalik Buterin, 1:49 https://youtu.be/I9dpjN3Mwps

5. If the value transfer failed because the sender did not have enough money, or the code execution ran out of gas, revert all state changes except the payment of the fees, and add the fees to the miner's account.

6. Otherwise, refund the fees for all remaining gas to the sender, and send the fees paid for gas consumed to the miner.

– Ethereum whitepaper[63]

The Ethereum cryptocurrency, ether, doubles as **gas** to incentivise computation and prevent certain attacks, and transactions double as **messages** to call a change to the stored data in contract accounts. In this sense, transactions are used to 'fuel' computation in the Ethereum blockchain. In order to facilitate the use of ether as fuel to run computations, the design of the Ethereum currency differentiates from the Bitcoin deflationary model (with the absolute cap of 21 million Bitcoin), instead steadily increasing ether in circulation. 'We view Bitcoin to be kind of like gold, and Ethereum to be more like oil in terms of the economics and how we have designed the system' (Hoskinson, ex-Ethereum developer).[64] If an increasing amount of computation is to be run on the platform, it requires there to be an increasing amount of ether to 'fuel' these. One of the curious aspects of the Ethereum architecture is the concept of 'gas price'. The motivation for introducing a **gas price** was that in order to make the Ethereum platform Turing-complete (and thus a generalised platform), there were certain computational functions that had to be made possible, including loops.[65] Loops, as the name suggest, can be written to run infinitely, and can thereby be used to delay or prevent other transactions and computation from running by busying miners with infinite loop computations. As a security measure against infinite loops, or for that sake any kind of DDoS attack, the concept of **gas price** was introduced, in which each byte has a price that needs to be pre-paid in order to be mined and validated, by including a given amount of ether (gas) in the transaction.[66] (On a more conceptual level, the gas price might therefore be understood as a limit to the Turing-completeness of the platform). Price mechanisms are used as a way to put limits on the use of resources in the network – a concept of using cost for securing decentralised networks that can be traced back to Cynthia Dwork and Moni Naor's 1992 paper suggesting price as a means to combat junk mail (Dwork and Naor, 1992), via Back's Hashcash and proof-of-work in Bitcoin. The implications of this were to become very complex as market dynamics were integrated deep into protocol designs and inspire a field of research that has been given the name 'cryptoeconomics' (see 5.2.2).

[63] See https://github.com/ethereum/wiki/wiki/White-Paper [accessed 16.11.2016]
[64] See https://youtu.be/hdAnyC45ZbU
[65] In fact, all functions in the Ethereum Virtual Machine effectively run as loops and only stop when they have run out of gas.
[66] Gas price is also understood as a mechanism to discourage computational waste and encourage efficient coding.

To recap, then, how transactions, computation, state change and the blockchain operate in Ethereum: each new block in the Ethereum blockchain represents a **state transition**, i.e. a transition from one state of accounts to another. It is **mined** in a similar way to Bitcoin, using the **proof-of-work** algorithm (with plans to change to what is called **proof-of-stake**, discussed further below). Any computation that changes data associated with accounts implies a state transition in the blockchain and costs **gas,** which is paid to the miner. In other words, transactions can either be transactions of ether from one external account to another, or ether as 'gas' that sparks some contract code, changing its stored data implying a state transition in the overall network to be included in the next block to be mined on the blockchain and verified by full nodes. A contract account's code might also be composed, in the **Solidity** language of '`constants`', which is essentially computation that does not involve any changes to the data of a contract (and can therefore be run without the need for mining).[67] A '`promise`' on the other hand implies computations where there is a change in the data. State transitions to any given contract are verified and executed across *all full nodes* that have validated that contract account:

> `the process of executing contract code is part of the definition of the state transition function, which is part of the block validation algorithm, so if a transaction is added into block B the code execution spawned by that transaction will be executed by all nodes, now and in the future, that download and validate block B.`
>
> – Ethereum whitepaper[68]

In order to understand the particular reasoning and attraction of a network where each node runs the same computation, essentially operating as a large inefficient network, I need to explain the Ethereum Virtual Machine.[69]

Ethereum Virtual Machine

The Ethereum Virtual Machine (EVM) is how computation is executed in a decentralised manner across the network of miners and full nodes. Miners compete to mine blocks containing the state transition along with transactions. Full nodes, in a similar manner as in Bitcoin, verify blocks, which also entails computing the state transition to check if the results submitted by the miner are correct. The miners compete in running a given piece of code,

[67] From the blogpost: https://medium.com/zeppelin-blog/the-hitchhikers-guide-to-smart-contracts-in-ethereum-848f08001f05.
[68] See https://github.com/ethereum/wiki/wiki/White-Paper#blockchain-and-mining
[69] It is worth mentioning here that, similarly to Bitcoin, the concept of 'each node' running the computation should be qualified, as the network has emergent tendencies and nodes begin to specialise. New techniques, for example what's known as 'sharding' are also worked on in order to allow networks to split the workload so to speak, but without compromising on the security intentions of decentralisation – namely that no aspect of the network is in control.

incentivised by receiving transaction fees and gas price, paid to the first miner to execute a given computation. Because many miners might be competing to compute the same code, which is then computed again and verified by full nodes, the EVM could be understood as a hugely inefficient decentralised computer. However, its purpose is not to aggregate computing power and create a large supercomputer, but rather to ensure 'trust' in a given computation, understood in the sense of not relying on a trusted intermediary, but conducting the computation again to verify it. It is an unfamiliar mode of thinking about a computer system, where efficiency and speed are the usual metrics, but unpacking the histories and motivations for this architecture in notions of trust, decentralisation and network security research gives a better understanding of the motivation for such a system in which the EVM serves a very particular function as a layer that facilitates and secures a particular kind of trust.

The use of the EVM and the relationship between trust and computation was illustrated to me in the following example by a mathematician and Ethereum enthusiast participating in the Bitcoin Summer School in Corfu 31st of May 2016: say you wanted to find out the voting results in an election. Such a computation, if run on the EVM, would be hugely expensive in terms of gas price as you would have to pay for the EVM to run as many computations as votes, +1 for each candidate, for each vote cast. Instead of this expensive and inefficient method, the question could be written as a Smart Contract promising a reward for the results. The computation could then be run by anyone 'off-chain' on a person's local computer, who would then submit their results to the Ethereum blockchain. In the case that different people submit different results, the EVM can run the computation to determine who submitted the correct answer first (who would be rewarded) and punish those who submitted the wrong answer, making it expensive for anyone to submit false results. In this sense, the EVM can be used as a type of arbiter of last resort, a threat that is only invoked in case of conflicting results, or to put it differently, a crisis of trust.[70] The intention is that other miners have the economic incentive to run the computation locally themselves and check if this is in fact the correct answer because they can reap the reward if it is incorrect, and on the other hand anyone submitting a false result runs the risk of paying for the full computation by the EVM. The applications of Smart Contracts and the use of the EVM are therefore of a particular kind addressing, specifically, questions of trust and truth in the form of calculability, insurance and rewards. In the following I go into a few more of the intended uses of Ethereum and how a particular network security understanding and concern for 'trust' would lay the ground for contracts and organisations that are intended to be beyond human control and determinacy.

[70] Note that whoever submits the computation to be solved might want to submit their own answer to the computation, to avoid zero answers and therefore having to pay for the EVM to compute all the computation loops.

4.2.2 Non-human determinacy

> This is the difference between me and Mark Zuckerberg. I live in a world where I presume that I could be a potential adversary to the system.
>
> – Vitalik Buterin, interviewed by Hans Ulrich Obrist, 2018[71]

As Buterin describes in the quote above, the core of the proposition of the Ethereum platform was the idea of 'trustlessness' that the system is secure and runs autonomously, even from the inventor himself. With Ethereum, the blockchain was no longer envisioned as the architecture for a new type of currency but 'generalised' to be able to run any type of computation. The importance of Bitcoin had shifted to represent the possibility of an apparatus that would organise a decentralised network without the need to resort to authority. The idea of authority tends to refer to some powerful corporate, financial or state entity that looks to control the networks for censorship, sanctions, surveillance and control. But in decentralised systems design, authority takes on a slightly different and expanded meaning, namely referring to *any* potential aspect of the system that the system as a whole is dependent on. This, from a security perspective, makes sense, because if there is any part of the system that it as a whole depends on, this can, in turn, be a target for such external authority. It, in the meantime, gave rise to a particular idea of trust and trustlessness that centred on the corruptibility of human judgment in general. No aspect of the system should be fully trusted and no human relied upon. This connected ideas of censorship-resistance and anti-authoritarian efforts with the idea of the necessity for a system beyond the control of humans. In the meantime, such ways of thinking about and designing 'trust' (see the EVM example above) in protocol and application design were highly unusual in terms of more general applications, without very clear use-cases. In order to give some sense of what this new platform might be used for, inventor of Ethereum, Vitalik Buterin, in his launch presentation, outlined three potential areas of experimentation and development: decentralised applications (dApps), Smart Contracts (originally articulated by Szabo, 1997) and Distributed Autonomous Organisations (DAO).[72] Here I discuss some of these applications and their motivations.

Unstoppable applications and Smart Contracts

On the landing page of the Ethereum platform, the tagline was 'build unstoppable applications' (see *fig. 4* below). By 'unstoppable applications', what is meant is that the decentralised application is hosted and run on a network and can therefore not be controlled or shut down by any single actor or authority. The idea of decentralised applications (dApps)

[71] See https://tankmagazine.com/issue-74/features/vitalik-buterin/
[72] See https://youtu.be/l9dpjN3Mwps

is to ‘disintermediate’ the running of online applications such that they are not run from any single server but instead are run across the network. The idea followed that this had the potential to disrupt existing platform services, like Facebook, AirBnB or Uber, and make it possible to instead operate and remunerate such services in a decentralised manner. The understanding of and reasoning for this particular kind of disruption are discussed in-depth in Chapter 5, while here I discuss how such ideas are sought to be realised in protocol designs.

Figure 4. ‘Build unstoppable applications.’ Screenshot of Ethereum landing page, August 2017.

The expansion of the remit of blockchain in Bitcoin from currency systems to any potential application on the basis of decentralisation suggested the possibility of resolving the role of authority in other affairs, and Ethereum sought to address, in particular, law and governance. The programming language of the platform is described as ‘contract-oriented language’ and code run on the platform is generally understood and referred to as contracts being executed, an explicit reference to and further instantiation of the notion that ‘code is law’ (Lessig, 1999). In order to run a decentralised Uber, for example, there would need to be a way to specify and enforce terms of use without resorting to an ‘intermediating authority’. Smart Contracts would be the solution: the contracts are written in code and therefore immediately executing without the need for external enforcement after the fact, and the contract code is held in the network and therefore cannot be tampered with or be modified after the fact. The ‘Smart’ in a Smart Contracs refers to the notion that the contract is self-executing, and it is so on the basis of that it executes on the decentralised network whenever it is prompted to, by either a person, or another contract account, sending it ‘gas’. Once written and deployed, it executes exactly as written, regardless of human intent or attempted control, including that of the original author. The ‘contracts’ aspect of Smart Contracts is essentially a re-conceptualisation of computational code. It is a conceptualisation that has significant effect in that calling bits of

code ‘contracts’ immediately directs attention and efforts towards the development of particular types of functionality in which relationships are primarily understood and encoded as contractual and transactional.[73] The Ethereum Smart Contract coding language is called Solidity, an example of which looks like this:[74]

```
pragma solidity ^0.4.0;
contract Counter {
      int private count = 0;
      function incrementCounter() public {
            count += 1;
      }
      function decrementCounter() public {
            count -= 1;
      }
      function getCount() public constant returns (int) {
            return count;
      }
}
```

– Gerald Nash, counter Smart Contract[75]

The contract code here specifies the type of contract, namely a `counter`, and that the counter contract has three functions: `incrementCounter` that increments by 1; `decrementCounter` that subtracts 1; and `getCount` which returns the total count at any given time. On its own this is not the most useful contract (and as mentioned in the example describing the EVM above, it is not either the most effective way of counting in the network given that each increment needs to be paid for). However, it gives a sense of the kinds of contract building blocks and the accessibility of the Solidity syntax. It is relatively easy to write and deploy contracts and there are well-documented guides and introductions that non-developers can also follow. The more difficult aspect is understanding what particular use-cases might benefit from being run in a decentralised manner and through such notions of trust, contracts and transactions; how to achieve an aim in the most efficient way given that each computation has a gas price; to understand the relations between clusters of Smart Contracts, their implications beyond those contractual relations; and to ensure that these are actually secure. Once deployed on the Ethereum blockchain it is near impossible to reverse or change what has been written. This is a core feature of the platform, part of what makes dApps ‘unstoppable’, Smart Contracts ‘self-executing’ and, as explained below, Decentralised

[73] This is part of a broader effort in coding communities to develop languages that are closer to human languages to encourage more engagement and literacy in how things are developed. So in addition to Solidity, Ethereum is also using a ‘natural specification format’ to clarify what is triggered by different aspects of Smart Contracts. See https://github.com/ethereum/wiki/wiki/Ethereum-Natural-Specification-Format
[74] See https://solidity.readthedocs.io/en/develop/
[75] From https://gist.github.com/aunyks/22be27444d6a9a91d2305c2ea2e2f7e8

Autonomous Organisations 'autonomous'. As it turned out, not being able to modify contracts can have severe implications (explored at length in Chapter 6) and be tricky for many uses, requiring other layers of more editable elements (discussed in Chapter 5).

The idea of Smart Contracts predates Ethereum and Bitcoin. Their initial articulation is assigned to Nick Szabo and a blogpost he wrote in 1997, *The Idea of Smart Contracts.*[76] Szabo also outlined a dedicated Smart Contracts language in 2002 that 'models the dynamics of contract performance – when and under what conditions obligations should be performed.' Contract-oriented languages tend to prioritise clarity such that people can understand the contractual relations and what conditions might trigger which aspects of the contract. But contract-oriented languages, and the obligations and conditions that are envisioned, tend to prioritise a certain *type* of contractual relations, often related to securing property and determining access. Already in the initial conceptualisation of Smart Contracts in 1997, Szabo uses the example of a lock to demonstrate the potential uses and a set of contractual relations determining payment conditions for a car:

> we've gone from a crude security system to a reified contract:
>
> ```
> (1) A lock to selectively let in the owner and exclude third
> parties;
> (2) A back door to let in the creditor;
> (3a) Creditor back door switched on only upon non-payment for a
> certain period of time; and
> (3b) The final electronic payment permanently switches off the
> back door.
> ```
>
> – Szabo, 1997

It is not a coincidence that many examples of practical uses of Smart Contracts, and in fact the very first Ethereum-based company, Slock.it, focused on connecting physical locks to the platform to use Smart Contract to determine criteria of access.[77] Cryptography is a technology for determining access; initially, access to messages with the aim of securing and verifying these and ensuring privacy of communications. With Bitcoin, messages implied transactions, and cryptography became primarily a means to secure property. If indeed Ethereum was to facilitate decentralised versions of AirBnB, Uber and so on, then there would need to be some way of extending code as law to physical space. Founded by three previous Ethereum developers, the company Slock.it produces blockchain-based applications for managing things to 'Rent, sell or share anything – without middlemen.' (Slock.it, 2016) The company combines developments in the Internet-of-Things with Ethereum Smart Contracts in order to

[76] See http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html
[77] https://slock.it/

realise the promises of Smart Contracts beyond a purely digital realm. In order for the claims of Smart Contracts to hold true as self-executing in relation to physical relations and property required some further effort and elaboration, combining 'smart property' with Ethereum Smart Contracts, so that, for example, a lock determining access to a physical space or thing might be unlocked through an ether transfer from one account to the other.[78] In order for Ethereum to realise the promise of trustlessness, to be a platform without authority, it would need to be beyond the control of humans who might otherwise be corruptible and therefore require some mediation. This notion runs through the envisioned uses and application of the platform such that dApps and Smart Contracts would also run beyond anyone's control, determined and executed in a decentralised manner through code. Such an 'disinterested algorithmic interpreter' (Wood, 2014a, p. 1) would also have to be able to operate in the physical realm in order for many applications to make sense, and would therefore require the expansion into locks and physical objects, in the meantime giving rise to the idea of things that own themselves. Otherwise the execution and enforcement of Smart Contracts would once again depend on external, human-based authorities. What I have described here is the way that the idea of trustless systems, once generalised, demanded an expansion of such non-human, algorithmic modes of determinacy in order to remain consistent with the vision of resolving the need for authority through a generalised, 'transaction-based state machine' (Wood, 2014a). The idea of 'trustlessness' had in this sense, through its generalisation, laid the ground for the need for such things as Smart Contracts and unstoppable applications that would operate autonomously from humans. This, in the meantime, also necessitated expansions of such algorithmic modes of determining relationships and access to physical objects and an increasing number of relationships in order to hold true. This also inspired the idea of entire organisations and corporations formed on the same basis of 'trustlessness'.

Decentralised Autonomous Organisations (DAO)

> Historically, corporations have only been able to act through people (or through corporate entities that were themselves ultimately controlled by people). This presents two simple and fundamental problems. Whatever a private contract or public law require: (1) people do not always follow the rules and (2) people do not always agree what the rules actually require.
>
> …While bad behaviour may make a corporation or its management civilly or criminally liable, punishment can come as little comfort to an investor who has already lost their money.
>
> – DAO whitepaper, Christoph Jentzsch, 2016

[78] See http://szabo.best.vwh.net/formalize.html and Szabo, 1997 for early definitions of Smart Contracts.

This brief quote from a whitepaper by Ethereum developer and co-founder Christoph Jenztsch neatly captures the problems that an Ethereum DAO contract is supposed to solve, namely rules (Smart Contracts) that execute as written, independently of any person's individual will or control (solving the 'problem' of people not following or disagreeing with the interpretation of rules), and the `splitDAO` function, allowing investors to take their funds with them to a new DAO if they disagree with the direction taken – solutions and interpretations of problems that were to turn out hugely problematic when put into practice. Here I briefly explain how a DAO is intended to function, a further attempt at operationalising ideas of 'autonomous' as meaning beyond human control, which also lays the technical ground for understanding how things went wrong in the first ever explicit attempt at a DAO (see 6.2.2).

A Decentralised Autonomous Organisation (DAO) is made up of a cluster of Smart Contracts. DAOs are meant to run according to a set of pre-written functions, rules and operations, independently of which humans or interests might otherwise interpret or try and change it. While there exists varying perspectives of what a DAO might or should be, with some suggesting that Bitcoin itself is already a DAO, the most comprehensive definition and practical instantiation to date is presented in the Ethereum DAO contract code (https://github.com/slockit/DAO), based on a whitepaper by Slock.it co-founder Christoph Jentzsch, (Jentzsch, 2016). Another extension of the notion that Bitcoin presented a decentralised resolution of authority, the focus here was on governance and the possibility of incorruptible governing protocol by ensuring that the governance rules could not be tampered with.[79] The idea is that organisational governance can be fully automated and the motivation for this is to solve the issue that Jentzsch lays out in the quote above – 'people do not always follow the rules' and 'people do not always agree what the rules actually require' (2016). This reasoning, in which disobedience and varied interpretation are understood as a problem to be solved through concise and automated code, has since The DAO whitepaper been widely problematised through experiences of implementations as well as research (cf. Levy, 2017) reminding the community that vagueness is a very useful feature of law and organisational management, allowing for these to function in the face of contingencies and unforeseen events.

The meanings of the words 'decentralised', 'autonomous' and 'organisations', while conjuring all sorts of political and ethical positions, are in fact actualised in quite specific ways in the architecture. It is important therefore to unpack what aspects of the architecture these concepts relate to and describe. 'Decentralisation' refers to the fact that the organisational rules are deployed and enforced on the Ethereum blockchain and run by the EVM, meaning a network of 'disinterested' nodes that run the computation associated with the DAO on the

[79] This tendency was to inspire statements such as Vinay Gupta's 'state in a box', see http://guptaoption.com/4.SIAB-ISA.php and projects such as Bitnation, see https://tse.bitnation.co/.

basis of financial reward. This is quite different from, say, decentralisation in the sense of people organising amongst themselves to take decisions in as a group rather than by one person. The notion of an organisation being 'autonomous' refers to the idea that the cluster of Smart Contracts sit on the decentralised network and executes as written without any person being able to modify it. It essentially means autonomy from the interpretation and control by any single human. Again, a very different understanding of autonomy than the idea of, say, political autonomy in which a group take control over and determine their own political processes and spaces. This is complicated by the fact that Ethereum does to some extent also address ambitions of political autonomy, being able to assemble and determine, as a group, one's own rules and processes by making the writing of rules accessible, their deployment forceful and secure. However, the idea of 'organisation' is also quite specific, determined on the basis of particular interactions and relations that do not resonate with many other forms of groups and associations: in DAOs, people engage with the organisation as either a **token holder**, which is very similar to a shareholder; as a **contractor**, which means you perform work that is commissioned by the DAO; or as the DAO **curator**, which has the responsibility to maintain the list of addresses that can receive ether from the DAO (as contractors, for example, or as returns on investment for token holders).

> The main contract is called 'DAO'. It defines the inner workings of The DAO and it derives the member variables and functions from 'Token' and 'TokenCreation'. Token defines the inner workings of The DAO Token and Token-Creation defines how The DAO token is created by fuelling The DAO with ether.
>
> – Jentzsch, 2016, p. 3

Tokens were initially intended as one of the building blocks of DAOs. Tokens in blockchain and cryptocurrency projects more generally have come to be understood primarily as speculative assets and a means to raise funds to start a new project (see 'Initial Coin Offerings'). But these were always also intended as a governance mechanism, inspired by their use for incentivising network contribution in Bitcoin mining, and representing both voting rights and a stake in decisions. The relationship between tokens, value, stakes and behaviour form a field that has been given the name cryptoeconomics (see 5.2.2). The focus is how the design and engineering of tokens in protocols might produce different security properties and is used for the development of new consensus algorithms. A DAO, as outlined in the whitepaper, was to operate as follows: first there is a DAO 'creation phase' in which anyone can purchase a token in the DAO by sending ether to the DAO contract account. Tokens represent a type of stake or share in The DAO, granting both voting rights as well as share in potential profits made by any work done for the DAO by **contractors**. A DAO cannot do much on the Ethereum Virtual Machine without ether and so the creation phase provides the

DAO account with funds to execute contracts. The ether is held in the DAO contract account, with the idea that the contract account on the blockchain guarantees the security of the funds independently of any special interest as it is governed purely by the contract account held in the decentralised network and therefore beyond the control of any one person. Token holders can freely trade their tokens on the Ethereum blockchain. Because the DAO itself cannot 'build a product, write code or develop hardware', it needs to hire humans to do so.[80] A person or group can submit a proposal to the DAO to become a 'contractor' and perform a task or piece of work. Contractors can be fired or replaced at any time by the DAO token holders through a voting process.[81]

The ambition of a generalised system beyond control keeps coming up against problems of how to interface with various non-algorithmically-determined conditions. Human meddling as well as new institutional forms keep creeping back in, and in the designs of Decentralised Autonomous Organisations this becomes painfully visible with the role of what has been named curators.[82] In order to secure the DAO from attacks by, for example, contractors submitting arbitrary proposals, the position of a 'curator' has been defined. The curator alone decides who can receive funds from the DAO by maintaining a whitelist of approved accounts. (It is worth repeating here that this description is based on the 2016 whitepaper by Jentszch and so should not be read as the current state of DAO development.) The curator comes close to being an authority, deciding which addresses can or cannot be paid to. This is resolved in two ways: the curator can be replaced following a two-step voting process in the DAO, and the voting process allows for the minority to potentially 'split' if unhappy with the result of the vote, taking their own ether stakes with them in a new DAO. The `splitDAO` function is an important aspect of the design, which was to have all sorts of ramifications, and is symptomatic of how differences more generally tends to be dealt with, both of which are discussed at length in Chapter 6. It also draws on another emphasis in the type of anti-authoritarianism in blockchain, namely voluntary involvement, whereby people contribute as and where they want to but also have the freedom to leave.[83] Decision-making is distributed and enforced by the contract code across a number of tokens and token holders, so that '(1) participants maintain direct real-time control of contributed funds and (2) governance rules are formalised, automated and enforced using software.' The ether funds of the DAO are in this sense under the control of token holders, but they are not able to modify the operations of the DAO as this is enshrined in what is advertised as immutable contract code on the blockchain. Another unresolved interface in terms of trustless architectures and algorithmic determinacy comes up in the use of Smart Contracts. In order for, say, a Smart Contract to release funds

[80] See https://www.ethereum.org/dao
[81] For a full description of how a DAO might operate, see: https://medium.com/@BlockByBlock/the-decentralised-autonomous-organization-dao-5e80cfe8c993#.zbcei3c0m and https://daohub.org
[82] See https://daohub.org/curator.html
[83] So-called 'voluntarysm' is one of the main aspects of a particular branch of US-based anarcho-capitalism subscribed to by amongst others one of the more famous Bitcoin entrepreneurs Roger Ver.

when certain conditions are met, this requires input of some sort. The sources of such external input are called **Oracles** and can be either a human or things like APIs and other external data feeds; a frequently mentioned example is the use of the BBC weather data feed for an insurance Smart Contract.[84] This example points to the limits of claims of trustlessness and disintermediation. In this case, even if the Ethereum blockchain could be considered entirely trustless, trust is nevertheless placed in the BBC weather data feed, entailing, indeed, again a reliance on a trusted third-party authority. Even if cryptographic proofs, the blockchain and cryptoeconomic systems might be considered entirely trustless then, the more such systems seek to incorporate into algorithmic modes of determinacy, the more surface is opened up to interface with all kinds of human and non-human sensibilities.

4.2.3 Non-human affinities

References to imperfect, unpredictable, potentially corrupt 'mushy humans' resonate from Bitcoin throughout aspects of Ethereum, as a project to realise a general platform whereby no human would be trusted or able to control it. It gave rise to a very particular notion of autonomy of the system, expanded through **Smart Contracts** to ideas of the DAO. Such ambitions are made to matter by for example making contract accounts on the Ethereum network able to 'call' functions in other contract accounts without the need for human prompting. As clusters of Smart Contracts and DAOs expand and interact with each other, systems of automated processes might set in motion in ways that can potentially develop way beyond immediate oversight and understanding of humans, and in ways that, in theory, would be unstoppable. These ambitions also provoked speculation about what might happen when cryptographically unbreakable, self-executing blockchain systems might be wielded by a future artificial intelligence. From the very beginning of Ethereum there was therefore a giddy self-conscious excitement about possibly creating an unstoppable algorithmic authority, questioning whether the platform represented a 'freenet or Skynet' (Filippi, 2014).[85] So far, actual implementations have turned out to be more mundane, looking towards efficiency gains of automating aspects of contracts and payments, and not quite able to fully sever the ties to the mush the insensible and indeterminate. Yet there are tendencies in the community that actively strive towards such a realisation of a system with its own agency. The rationale is in part that such an agency might provide a form of governance, legal and economic substrate that would be more rational and objective than any human or human-based system might. This disinterested algorithmic substrate would facilitate all manner of rules, currencies, organisations, differences and projects, and in this sense be beyond the political, because it would be able to facilitate any kind of systems design. At other times, such perspectives of

[84] New companies are springing up to serve this market of feeding dApps with data, amongst others Oraclize http://www.oraclize.it.

[85] Skynet refers to the AI group mind in the Terminator films that gained self-awareness and decided to eliminate humanity after concluding that humans will inevitably want to shut it down.

algorithmic mediator take more sinister forms, arguing for why an agency constructed through mathematics and markets represents a necessary and inevitable evolutionary stage and the possible extinction of human beings as a result.[86]

Here, in particular, I want to draw in the cut of the *insensible* in order to disentangle and suggest a different ground for debate. When faced with such notions of the necessity of an algorithmic determining agency it is tempting to react by reasserting human responsibility, control and oversight. Yusoff, in her discussion of the insensible and the extinction of forms of life that are beyond sensibility, raises the question of the possibility of a response and responsibility towards that which has not been sensed, has not made itself matter to a specific sensibility. I want to argue that such a perspective might be valid and helpful for understanding not only forms of biological or mineral life beyond sensibilities, but also algorithmic agencies. To further expand on this, I will draw in what is perhaps an unusual take on ideas of AI and autonomous systems, namely animism. I want to suggest that anthropological studies of animism might provide some helpful ways of construing non-human aliveness in techno-scientific fields too. Studies of animism intersect in interesting ways with new materialism debates about how the material world 'matters' in ways that exceed assumptions of mute objects for the manipulation of humans. These imply that the 'aliveness' and forms of autonomy that are ascribed to such systems do not have to be fully adopted as inevitable (nor even necessarily important) but neither dismissed as speculative fantasy (and thereby assuming full control and agency with humans). Anthropological accounts of animism have since the '90s sought to re-describe animist practices in an attempt is to understand how 'aliveness' might be understood in specific ways and make sense within particular practices and contexts (Bird-David, 1999; Ingold, 2000, 2011). The emphasis is placed on relations and agency understood as exerting a particular force, mattering by literally making a material difference to a people or person. The specifics matter; *this* storm, *this* tree, *this* rock is related to as a being, because these have exerted some force putting them into relation with a person or a group. There is a relationship of some kind, whether malicious or not, and it therefore matters. This also means that what matters does not rely on some general description (not all storms, trees or rocks matter or are 'alive'), but is contextual (importantly for networked technologies, contextual here should not assume 'locality' necessarily).

Reading the form of autonomy implied in the ambition of Ethereum Smart Contracts and DAOs through these ideas is helpful in several ways. Firstly, it avoids the necessity to counter the idea of autonomous systems by insisting on human control and complete knowledge. Human control and complete overview of algorithmic systems are strenuous claims. Large

[86] I met such perspectives from individuals at meet-ups and developers' conferences in conversation. In some ways it is the logical extension of the idea of 'mushy humans', some going so far as to say that if some person was not able to effectively engage with blockchain systems and markets, they were of an inferior genetic strand that should probably die out.

network systems, and the operations of algorithms, indeed comprise elements that are beyond the immediate control, oversight and comprehension (Seaver, 2014; Amoore, 2015; Burrell, 2015). (And that therefore imply already existing practices of working with that which is beyond modelling and certainty). Secondly, the *insensible* and an animist understanding of relational aliveness also suggests that the affinities and relationships that are formed do not necessarily follow human versus machine narratives that tend to dominate imaginations for how autonomous systems might play out. To close off this chapter, then, I would like to expand a bit more on this second point and explain how recognising such affinities that cut across assumed lines between humans and 'the rest', along with the concept of the *insensible,* help to counter deterministic reasoning about the most appropriate agency of control, whether human or machinic.

The promise of an algorithmic, neutral determining sensibility that can be known, with mathematical certainty, to have certain properties, is simultaneously a promise of radical uncertainty, a machine necessarily beyond control, out of control. Operating beyond control suggests a particular 'aliveness' of an algorithmic determining agency, which then at the same time becomes necessary for the project of establishing a generalised, trustless platform. The two justify each other: a determining agency founded on indisputable proof cannot be controlled by any other agency or it would necessarily be tainted. In the engineering of a deterministic system, there is an awareness of aspects of the system, in particular how it plays out in practice that cannot be fully predicted or controlled. This is also the exact moment at which this aspect of being out of control conjures a certain 'aliveness' from this thing that is being built, a force that begins to shape aspects of the world that is not under direct command. This is all fine and well, and importantly, there are corrections; tuning, maintenance and changes that take place in the engineering of systems and protocols such that they begin to align more with the desired intentions and sensibilities. In fact, such tuning, corrections and maintenance reveal much of the desired intentions of such systems in ways that do point towards responsibility. But there is another problem, namely the necessity for the deterministic properties of such systems to be presented as universally mattering. The particular autonomy that is often articulated in Ethereum and Bitcoin is one that assumes universality on the basis of neutral mathematical determinacy. The autonomy and agency of Smart Contracts and DAOs might be considered real enough, in that aspects of these are indeed being built and might very well determine some things and act as a force in some people's lives. And yet, drawing on a perspective of aliveness from animism, such claims of aliveness do not allow for universal demands that this thing matters. From an animist perspective, and indeed from a radical Baradian interpretation, what matters depends on the sensibility that makes it matter, so to speak. And such sensibilities are not singular and universal, but rather multiple and, as Yusoff points out, also *insensible* (2013a). Drawing in Barad, blockchain might be considered one mode of determinacy amongst many in an

ongoing relationship with a field of indeterminate potential. This particular mode of determinacy matters significantly to some, but in no way has to be made to matter for others. The argument I am making then, is primarily a philosophical basis for the particularity of any algorithmic determining agency, as a prerequisite for assessing its particular qualities and assigning a rather limited role for such.

4.3 Conclusions

I titled this chapter *A politics for the insensible* in order to, on the one hand, point towards the importance of that which is not sensed as mattering by and in the development of a given determining apparatus, whether based on cryptographic proofs or otherwise. By suggesting a politics for the insensible, I want to make matter the haunting awareness that there is a limit to any given sensibility, whether constructed out of cryptographic proofs or algorithms trawling through and evolving in vast datascapes or otherwise, such that *insensible* aspects and beings might never make themselves matter to particular sensibilities. If the *insensible* is taken seriously, the unknown does not justify necessary expansion of a form of reasoning operating at larger scales, but instead becomes a reason for humility and limits. Such spaciousness, an 'affirmative action for the formless' (Yusoff, 2013a, p. 224), allows for affinities that cross human, machinic and otherwise non-human in ways that to some degree are already taking place but tend to be overlooked in attempts at making universal claims. Yusoff argues, in the context of her work on the anthropocene that 'human' as a category is historically fraught, and that indeed humans have been treated as resources to be extracted. This suggests that affinities and categories of 'human', 'nature' and 'machine' cross each other when it comes to questions and struggles over what matters. On the other hand, it suggests a more conscious articulation of those affinities, instead of assuming at each turn that 'humanity' as a whole is ever fully mobilised on one side or the other (for humans, against the machine or for the machine, against humans). Instead, with the help of Barad and Yusoff, I suggest a differentiation between, on the one hand, forms of blockchain assemblages that conjure the necessity of a singular organising principle and, on the other, those that acknowledge the limits to modes of determinacy – allowing a spaciousness for other forms of determinacy, for that which has not yet been sensed as mattering, and indeed the insensible that might never make itself matter.

In this chapter, I have described the Bitcoin protocol and the way in which it operationalises cryptographic proofs, decentralisation and economic incentives in order to suggest a method for determining consensus across a computational network. I have discussed how such a cryptographic mode of determinacy is proposed to resolve issues of 'trust', by replacing

human determinacy with that of a trustless consensus algorithm based on cryptographic proof – which, in the meantime, construes humans as necessarily subjective and untrustworthy, and cryptographic proofs as objective, the foundation for a trustless system. A Baradian approach does not necessitate one or the other to be the most neutral or objective and so instead of entering into a debate about whether human or cryptographic modes of determinacy are most appropriate in absolute terms, I describe and discuss necessary limits of a cryptographic mode of determinacy and the ways in which it construes other forms of determinacy as not mattering. I then describe and discuss the way the Bitcoin architecture, when deployed, has emergent dynamics whereby some of the claims of decentralisation and trustlessness come under strain, requiring maintenance and correction, once again pointing to the inseparability a 'pure' system from 'mushy humans'.

In the second half of the chapter I described the Ethereum protocol and intentions to make the Bitcoin architecture Turing-complete; a generalised platform for any computation. By extending the Bitcoin architecture, the Ethereum platform also extends ideas of non-human determinacy, which also brings with it a particular understanding of autonomy, namely as aspects of the system that would be beyond human control. Decentralisation and trustlessness is operationalised in order to achieve a form of autonomous execution of code in what are called Smart Contracts, and as autonomous organisational forms in Decentralised Autonomous Organisations. I discuss this suggested autonomy through ideas from anthropological studies of animism as a way to contextualise 'aliveness' and autonomy. I do this in order to suggest that instead of countering such ideas of autonomy by placing control and oversight back in the hands of humans, which to some degree cannot be taken for granted given both the emergent dynamics of network systems and algorithmic execution, that aliveness might be considered relational in these circumstances too. This means that a given networked system or algorithm might indeed be considered 'alive' and that there are indeed affinities between such systems and some humans, but that this is an expression of what matters for this particular community of people. It is a way in which to make such relationships specific, such that they can be discussed in their actual limited form, rather than assumed to have larger relevance as an abstract question of human versus algorithmic determinacy. With these architectures, protocols and forms of determinacy in mind, in the next chapter I trace these particular understandings of the concepts of decentralisation, trust and autonomy back to pre-Bitcoin histories of network technology in order to articulate the specific sensibility they are an expression of.

5 Blockchain sensibilities

In this chapter, I trace through events, experiences and histories of decentralised network technologies in order to describe what has given rise to a blockchain *sensibility* – sensibilities that indeed hold a blockchain assemblage together as a recognisable field. By sensibility, I refer to a general understanding, assumption and feeling for what matters in the assemblage, the tacit understandings of what is good or not, desirable or not. (The most obvious example of which is that 'decentralisation' is good and 'centralisation' is bad). The way I employ this notion of the sensible draws on Rancière's theories of the political as a 'redistribution of the sensible' (2010, pp.27-44) and Barad's onto-epistemology, whereby sensibilities, what is considered to *matter* and how it matters, in turn become part of a process of materialising new things (2007). The onto-epistemological cut that I draw, using this understanding of the sensible, is one that is concerned with the 'disruption' to existing sensibilities proposed by Bitcoin, Ethereum and blockchain and what came to matter for these assemblages in the process. Blockchain technology is described as a disruptive technology. But the question is what exactly makes blockchain 'disruptive'. Legal scholar Herian argues that blockchain should not be considered disruptive because projects have been brought in and play out well within the rules of existing capitalism (Herian, 2016). While I do not exactly argue against Herian's assessment, in the following I look to draw out and expand on what might be missing from this assessment: the diversity of already existing political and economic possibilities. I do this through a reworking of Gibson-Graham's notions of diverse economies (Gibson-Graham, 2008). Gibson-Graham propose a shift in attention, from a mode of analysis concerned primarily with capitalist advancement to instead give space and importance to already existing non-capitalist economic practices and the ways in which this diversity might be supported and expanded. Only if one addresses the world as entirely comprised and determined through capitalist relations does 'disruption' pertain only to projects explicitly articulated as anti-capitalist. In the attempt to draw out a blockchain sensibility, then, I make use of the notion of diverse economies firstly to open up a history and description that does not centre on questions of capitalism, but instead take seriously the ways in which blockchain has attracted people with a very diverse range of political and economic ideas. My main aim is to explain this, which, as it turns out, also effectively explains the ways in which capitalist tendencies, financial instruments and indeed technologies of state and legal institutions themselves are replicated in and through blockchain technologies in ways that simultaneously seek to disrupt these. In short, what matters to the blockchain assemblage is not exactly capitalism or anti-capitalism as such, but rather questions of decentralisation and centralisation that intersect with capitalism in certain ways, but are nevertheless operationalised through lived experience and an affinity with network computation.

The diverse economies approach is also helpful for opening up a sensibility *within* the blockchain assemblage, shifting the sensibility from the assumption of internal systems coherence to focus instead on the dependencies and relationships with other economic spaces. There is a tendency, from both within blockchain communities and more generally, to address blockchain projects and protocols in a hermetic manner, assuming that these can be assessed on their own terms. In the meantime, the significance of blockchain projects are always in relation to existing systems, not only because, just as everything else, they play out 'in the world', but more importantly because their very designs involve already existing economic systems. The field of cryptoeconomics is the most glaring example, whereby economic dynamics are incorporated into protocol designs in very direct ways, exchange rates being the most immediate. Exchange rates, for example, are rarely addressed as an explicit and deliberate condition of a protocol design, and are instead treated as an unfortunate side effect. A diverse economies approach suggests a shift in attention from assessing blockchain projects and protocols as hermetic systems, to instead focus on the interrelationships with other economic spaces and dynamics – not as a side effect, but as a lasting condition. This also counters ideas of blockchain systems presenting a wholesale replacement of existing systems, and instead acknowledging that, at best, they might present possibilities for some radical reconfiguration and, at worst, simply another layer of complexity to the already complex interrelationships of financial, political and digital systems.

The chapter is structured as follows: I first trace the particular understandings of one of the primary concepts in blockchain, namely *decentralisation*, through to earlier histories of decentralised network technology. By doing this I am able to articulate the more precise and particular understandings of decentralisation in operation in blockchain, namely as a strategy and a set of experiences of circumventing authorities through specific network architectures in the '90s and '00s. I then describe how these network strategies resonated more broadly with the launch of Bitcoin in the context of the financial crisis and the Wikileaks banking blockade, arguing that these contexts gave a new and broader meaning to this particular operationalisation of the concept of decentralisation. I argue that the *sensibility* of blockchain, in terms of what matters in the assemblage, the tacitly agreed-upon priorities, values and opinions whereby decentralisation is 'good', centralisation is 'bad' and so on, is primarily affiliated with network computation and such strategies for circumventing authority than any political or economic ideas. This, in turn, also brings with it a particular understanding of associated concepts of *authority*, *trust*, *control* and *autonomy*. I then describe more explicitly some of the main concepts in a blockchain political sensibility and the particular meaning and understandings associated with these. These concepts are not argued to be exhaustive, but rather present commonly used terms that cut across the field and many of the political differences within it. These are then discussed as they play out in and through two major events that suggested a broader appeal and relevance of Bitcoin, namely the 2008/2009

financial crisis and the Wikileaks banking blockade. In the second half of the chapter I discuss the generalisation of this sensibility in the launch of Ethereum. I discuss two main consequences of such a generalisation, namely its platformisation, and tokenisation of protocols, drawing out the ways in which these seek to be disruptive. The aim of this chapter then is to 'stay with the trouble' (Haraway, 2016) and attempt to articulate the precise nature of the emerging politics in and around blockchain technology with an aim of opening up new possibilities rather than arriving at a final assessment of its politics. The question the chapter seeks to address is what matters to blockchain communities, more specifically the Bitcoin and Ethereum case studies, and the events and contexts through which these came to matter.

5.1 Why decentralisation?

Decentralisation is arguably the main concept that informs a blockchain sensibility. In this section I begin by drawing out the motivations for decentralised architectures by tracing these through to pre-Bitcoin histories of peer-to-peer technology in the 1990s. These histories are helpful for articulating a more precise understanding of other key concepts used in the blockchain field, such as trust, openness and so on and their particular operationalisation in blockchain assemblages. Decentralisation was at the time a particular strategy employed for systems to be resilient to shutdown by authorities. With the launch of Bitcoin in the context of the financial crisis, I argue that decentralisation became generalised from particular strategy to a political proposition in its own right. The specific understanding of decentralisation in Bitcoin has been widely discussed and critiqued for its libertarian and right-wing references (Golumbia, 2016; Greenfield, 2017). Drawing on Gibson-Graham's notion of diverse economies opens up an appreciation of the more diverse interests, economic ideas and involvement in Bitcoin and the political possibilities that come with these.

I argue that the understanding and operationalisation of decentralisation is both broader and more specific than many critics of the politics of Bitcoin allow for: broader in the sense of appealing to a diverse political and economic spectrum and more specific in its particular affiliation to computational networks more so than political or economic ideology. I discuss the attraction of Bitcoin from several different monetary and economic perspectives as these were playing out in the financial crisis, arguing that the accommodation of such different political-economic perspectives is in part due to a political sensibility affiliated primarily with ideas emerging from peer-to-peer networks. I then discuss another major event that lent geo-political justification to Bitcoin, namely the Wikileaks financial embargo, and conclude that both of these events continue to shape the political sensibilities as well as imagined use-cases of blockchain projects to this date. Finally, I describe several of the key concepts

making out blockchain political sensibilities, suggesting a distinction between principles, properties and intended effects as a way to offer more clarity around these concepts and how they relate to technical architectures.

5.1.1 Disruption: networks vs. authorities

In a paper titled *Systematising Decentralisation and Privacy: Lessons from 15 Years of Research and Deployments* by a number of computer and information security scientists (Troncoso *et al.*, 2017), Bitcoin is analysed alongside, in particular, file-sharing system BitTorrent and anonymous relay network Tor as part of such longer history of decentralised systems. The paper assesses the application of decentralisation in systems, systematically reviewing different technologies since a 2001-edited volume titled *Peer-to-Peer – The Power of Disruptive Technologies* (Oram, 2001) which marked one of the first coherent overviews, narrative and reflections on decentralised systems at the time by many of the people building and maintaining these. Decentralisation, when traced through this particular history of peer-to-peer systems, is understood primarily and initially a strategy for circumvention, censorship-resistance and systemic resilience. The paper gives an important insight into the particular sensibilities around decentralisation as operationalised in and for peer-to-peer networks that resonate with and clarifies what otherwise might be considered curious lines of reasoning in subsequent projects like Ethereum – such as the necessity of systems beyond human control. Much of this history tends to be overlooked and is rarely explicitly discussed by both critics as well as proponents of blockchain systems, but are key to understanding the particular ideas and operationalisation of decentralisation in blockchain.

From their systematic review of decentralised systems design since 2001, Troncoso, Isaakidis, Danezis and Halpin define decentralisation as a subset of distributed systems that has the particular characteristic of having multiple or preferably no ‘authorities’ (Troncoso et.al. 2017). Distributed systems are resilient by having no single point of failure, meaning they can withstand unexpected faults, breakdowns or accidents, but the motivations for decentralised systems go further and are concerned with questions of censorship-resistance and transparency, considered to be features that are distinct to systems with ‘no authority’. Importantly, the concept of authority as understood in and for decentralised network systems is any aspect of the system that would provide someone/something full control and oversight of the network. The paper therefore argues for analysing any given protocol’s ‘authority topology’ in addition to network and infrastructure topologies. This distinction between ‘distributed’ and ‘decentralised’ is a way to differentiate between internet platforms and infrastructures such as Amazon, Facebook and Google, which employ distributed architectures but with particular commercial and governance structures that can determine the development of the platforms, and that governments would be able to pressure into for

example handing over specific information. Decentralised systems are in contrast intended to be out of the reach of any such authorities. The appeal and importance of such systems' designs can be explained more clearly through further examples of the intentions of pre-Bitcoin decentralised systems.

Since the late '80s and '90s there had been a string of other attempts at creating online cash, including DigiCash, founded by cryptographer David Chaum (Chaum, 1998), b-money, bitgold and E-Gold.[87] [88] [89] The early histories of these projects are, in many ways, prequels to Bitcoin, initiated on the basis of a concern for third party involvement in digital payments and looking to develop payment systems that would be untraceable by banks and governments. Chaum in particular was concerned with questions of privacy in online payments, keenly aware that commerce on the internet was likely to expand rapidly, and that this would bring with it a number of privacy problems. Douglas Jackson, the entrepreneur who founded E-Gold, was more concerned with critique of central bank issuance of money and providing a platform for non-state controlled and borderless transactions. DigiCash eventually went bankrupt and E-Gold was shut down in 2009 when, the founder was arrested by the FBI and was charged with money laundering and conspiracy, seemingly despite attempts at cooperating with the law.[90]

These experience and a growing politics of anti-authoritarian politics applied more generally amongst communities adopting peer-to-peer strategies. Peer-to-peer file-sharing networks were frustrating music, film and other intellectual property-based industries but also facing severe legal cases; information leaks by amorphous hacker/hacktivist groups were undermining corporate and government control of information (Coleman, 2009, 2014) and decentralised networks of servers and websites were facilitating independent news outlets, challenging monopolies of news and knowledge.[91] [92] One of the lessons that was gathered from these experiences was to not provide any single point of failure – whether server or person – that a government or any other authority or attacker might target in order to take down the whole system. Similarly, when the music sharing platform Napster was shut down on the basis of copyright infringement, BitTorrent became the decentralised answer, a file-sharing system that would enable people to share bits of files from many different sources in ways that were difficult to trace and therefore difficult to prosecute (Oram, 2001; Troncoso *et al.*, 2017). Decentralisation was rapidly becoming a strategy that was very much part of

[87] See http://www.weidai.com/bmoney.txt
[88] See https://unenumerated.blogspot.com/2005/12/bit-gold.html
[89] See for example https://www.zerohedge.com/news/2013-11-29/e-gold-founder-launches-new-gold-backed-currency
[90] See https://www.wired.com/2009/06/e-gold/
[91] cf. Napster, The Piratebay, the story of Aaron Swartz; (Terranova, 2004) Libraryoftheworld; Terranova, 2010.
[92] These groups included the Indymedia network using the Internet to take independent control of information, but which since has transforming into the plethora of blogs and self-publishing platforms and news distribution sites, and eventually into what we call social media today.

'network culture' more generally (Terranova, 2004; Coleman, 2009, 2014), a pragmatic systems architecture and organisational principle used for circumventing legal and political authorities.

The concept of authority and decentralisation began to be understood in terms that were specific to these experiences. Decentralisation implied systems in which no single element would be trusted; it implied 'disintermediating' third parties or anyone/anything that might be an authority or targeted by one. An 'authority' in the meantime would be any aspect of the system that would make it vulnerable to shutdown, so 'decentralisation' implied a system that is censorship-resistant and resilient to shutdown by having multiple or no authorities, such that the system would not be vulnerable to any single authority. Arrests and harsh sentencing solidified a more general anti-authoritarian politics, while the ability to keep systems running regardless lent a political fascination and affiliation with decentralised systems as able to withstand attacks by government and corporate actors (Coleman, 2009, 2014). Decentralised architectures proved effective as a means to protect the systems themselves from authorities, but in the meantime, those using it would still be arrested, prosecuted or face other kinds of consequences. This pre-history is very effective for understanding the particular meanings of concepts used in the blockchain space, and the experiences informing the particular sensibilities at play. It is also very helpful for explaining some of the main issues with blockchain, namely its peculiar characteristic of drawing interest and attention on the basis of its architecture itself, rather than its immediate usefulness (what Golumbia interprets as an excess of ideology (Golumbia, 2015)); a tendency to affiliate primarily with the interests and conditions of the systems design assuming these to extend to those using it; and the strange quirks that come from generalising the idea of trust and trustlessness from network security to a political proposition in its own right (see Chapter 4). In the following, I attempt to more explicitly articulate key concepts and their meaning within a blockchain context – a blockchain *sensibility,* so to speak.

5.1.2 What came to matter

Many of the words and concepts that form a blockchain sensibility can be traced to very specific experiences, reasoning and histories in network computation. Most of the concepts are, however, also broad enough to refer to and open up more general social and political imaginaries. This has effectively attracted a broad spectrum of people, discussed further below, but has also caused significant confusion. For example, 'decentralisation' can refer to a network type, but equally to what might be the assumed social and political effects of these. It is further complicated by the fact that decentralisation is not a stable condition. It can be contended to state for example that Bitcoin *is* decentralised, but it is nevertheless intended to be to such a degree that decentralisation operates as the main principle in the assemblage,

and is corrected for and addressed when not satisfied (cf. Meiklejohn, 2018). Whether strictly true or not in terms of the state of the network, decentralisation might operate effectively in a social sense, such that, for example, miners might hesitate to exert their rather centralised hashing power for fear of backlash (see 6.1.2). While the intention, as discussed in Chapter 4, has been to eliminate vague human interpretations by encoding conditions into immediately executing protocols that cannot be controlled, these principles and concepts nevertheless continue to operate, informing ongoing decision-making in the space and forming the rationale for different legitimacy claims (see Chapter 6).

Here, I attempt to clarify some of these confusions around the scope, claims, aims and ambitions of blockchain by doing three things: describing some of the main principles and concepts that form blockchain sensibilities; describing their particular meaning and operationalisation in terms of decentralised network protocols; and suggesting a distinction between general principles, particular desired properties and the hoped-for effects of Bitcoin and blockchain systems. These are in no way exhaustive, and the method for which I have arrived at the listed principles, properties and effects is far from structured or comprehensive. Instead, they are summations made on the basis of my involvement with the blockchain industry between the years 2014 and 2019 and should instead be read as navigational tools for the rest of the chapter, which will discuss some of the complexities and problems that come up when such a sensibility is generalised from a particular set of strategies in earlier histories of peer-to-peer structures to a generalised proposition (as well as the next chapter in which some of these sensibilities were severely challenged). What I here call blockchain 'principles' entail assumptions about what kind of systems and architectures will have certain properties and achieve different effects. These can be considered 'first principles' in the sense of that they are often used as indisputable, as a common understanding of generally desirable conditions in and of themselves. They are principles for which there is a vague albeit general consensus, and tend to form the fundamental reasoning and purpose of blockchain systems and that hold together the blockchain assemblage.

Decentralisation

Decentralisation is the main principle in blockchain and cryptocurrency efforts. While distributed systems imply that there is no single point of failure, the intention for decentralisation is to go further and ensure resilience against shutdown by authorities, censorship, influence or manipulation. The principle, defined in terms of resilience towards authority, also raises issues about whether not only the network, but also the developers who write the protocols, the distribution of bitcoin tokens in the network, hardware provisions etc. needs to be decentralised in order to satisfy the aims (Bonneau *et al.*, 2015; Srinivasan, 2017; Azouvi, Maller and Meiklejohn, 2018). Decentralisation tends to be understood through ideas of network topology and

assuming social effects will follow, but these ideas are increasingly adopting social and political sensibility of decentralisation in response to internal crises in the communities (see Chapter 6).

Openness

In order to not have any 'authorities' in a decentralised system, strictly speaking the systems reference client code has to be open source, so that it can be peer-reviewed and checked. If not, the persons who have written the code would effectively have to be trusted; no one would be able to check whether the system operates as stated, whether there are security issues or otherwise. Bitcoin and other decentralised systems like BitTorrent take openness further, also implying that anyone can take part in running the client and participating as a peer. They are designed so that anyone can join or leave as and when they want. 'In a decentralised system, no one entity can act to censor transactions or prevent individuals from joining the network (as is possible with traditional institutions...' (Azouvi, Maller and Meiklejohn, 2018, p. 1). This form of openness has technical, social and political economic implications because if anyone can join then it also needs to be assumed that anyone might be an adversary and look to attack the system. This implies a 'trustless' security model that has gone on to also become a form of social, political economic approach to any manner of systems designs that also configures ideas of neutrality in particular ways.

Trust/trustlessness

Decentralised and open systems imply a certain level of trustlessness. Trust in the context of network computation refers specifically to a security threshold, namely which percentage of a network have to be trusted and are assumed to be 'honest' for any given system. The ideal is to reduce the amount of trust needed as much as possible, approaching complete trustlessness and security. Bitcoin and many other blockchain protocols consider 51% attacks, whereby if anyone controls 51% of the network, they would be able to determine which transactions are verified and compromising the neutrality of the network. This conception of trust, while effective in systems design and security modelling, meets severe contradictions when the systems are actually deployed, and the levels of trust required for their use and deployment (Vidan and Lehdonvirta, 2018)

Immutability

The Bitcoin blockchain would have to be immutable in order for it to be secure. Otherwise, anyone could change the record of accounts, rendering the system

useless. Immutability would secure that consensus on the state of the network, arrived at through the proof-of-work consensus protocol, and could not be arbitrarily modified. This idea of immutability was extended in Ethereum to the blockchain more generally and the idea of immutable code – code that would run exactly as written, that no one could change and that therefore would run and function 'autonomously' beyond the control of any human. Immutability was a main principle in blockchain systems until it became severely challenged after a series of hacks in 2016 and 2017 (see Chapter 6).

To appreciate the specificity of these principles, it can be helpful to compare them with what such notions might refer to in other contexts. For example, social and political understandings of decentralisation might aim at bringing control and decision-making closer to those who are affected by a given decision, while in the case of aspects of blockchain decentralisation, the systems are designed specifically so that they are beyond the control of any given person, whether or not they affect them. Equally, social and political understandings of trust might consider more trust to be a good thing, while for anyone looking to model and develop secure network systems, any trust required in the network represents a potential attack vector and a weakness. Because of this, the kind of openness that is implied is of a particular nature, where, in terms of social life, one might associate openness with a trustful relationship to others. In decentralised systems, openness is based on precisely calculated security threshold, implying and assuming that anyone might be an adversary. This concern of first and foremost with security and the security properties of different design principles, when generalised, tend towards securitising and militarising of how relationships are modelled and determined more generally. They are intended to withstand attacks from any potential source. The provenance of these concepts in network security concerns were to go on to affect the ways in which neutrality is understood in relation to political difference (expanded on in section 5.2.1).

These principles are, in turn, associated with particular *properties* that are generally considered desirable in blockchain systems. Such properties are specific to a given systems design and can be achieved, but are not necessarily guaranteed, by following certain design principles. The ones described here are some of the more general properties that different blockchain projects try and ensure for people using them. Again, these are not exhaustive in any way, but are intended to give an overview of the types of concerns that blockchain systems designs tend to take into account, which also gives a sense of what matters in blockchain assemblages in terms of use-cases and needs. They are therefore often seen as the reasons for what are called **forks** of existing projects (see 6.2.1) or the development of

entirely new projects, cryptographic or mathematical tools that suggest new and better ways of achieving such properties.

Privacy

Privacy is one of the most prevalent properties and concerns in early decentralised systems designs and in Bitcoin. It is a politicised field of computer engineering that tends to be the focus of activists' development efforts in the realm of information security (cf. Rogaway, 2015). It is a property of systems designs that became the focus and reasoning of what is called Cypherpunk, a political movement and subculture that seeks to use cryptography as a counter measure against authority. Cypherpunk is, in many ways, the political and cultural backdrop to Bitcoin. From very early on in the development of the internet, a network of engineers and developers were concerned with the ways in which the system would fundamentally alter power relations between governments and citizens. Privacy was considered a crucial point and the focus of two manifestos that came out of Cypherpunk movements: a Cypherpunk manifesto by computer programmer and founder of the Cypherpunk mailing list Eric Hughes, stating for example, *'Privacy is necessary for an open society in the electronic age'*, *'Privacy is the power to selectively reveal oneself to the world'* and *'We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.*[93] [94] Another contributor to the Cypherpunk mailing list, Timothy C. May wrote the crypto-anarchist manifesto that begins with *'A spectre is haunting the modern world, the spectre of crypto anarchy. Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner.*[95] These concerns predicted what has since become more a prevalent understanding of the internet as having become a mass surveillance infrastructure. On a more technical level, the intention is that peer-to-peer technologies intersect with privacy properties by eliminating third party intermediation that would otherwise have full oversight of behaviour and data. In some peer-to-peer designs, however, third party intermediation is replaced with a different kind of decentralised intermediation in the shape of the protocol itself. And so in Bitcoin, in order to have a peer-to-peer payment system, instead of a third party holding a record of transactions, the whole network holds it, making all transactions fully public. In order to preserve privacy in such a

[93] See archive here: http://mailing-list-archive.cryptoanarchy.wiki/
[94] See https://www.activism.net/cypherpunk/manifesto.html
[95] See https://activism.net/cypherpunk/crypto-anarchy.html

radically transparent system, the accounts themselves remain anonymous. Privacy is a desired property of decentralised systems, but its design is never absolute, instead entailing decisions around selective revealing and concealing of relevant information and very careful modelling of potential systems weaknesses.

Anonymity

Anonymity is closely related to privacy, but slight different in terms of systems design. A given user or node might be anonymous but still engage in open and non-private communication. This is also a major aspect of Cypherpunk and network culture with a fascination and use of pseudonyms and 'nyms' conveying the possibility of multiple identities and the ability to selectively reveal or conceal oneself. Bitcoin was initially understood to be anonymous, and infamously became the means of payment for the 'Darknet' and online black markets (cf. Pagliery, 2015). The anonymity and subsequent disappearance of Bitcoin inventor(s) Satoshi Nakamoto was in the meantime also a symbol of the disappearance of authority. The author of the system receded into the shadows, the 'nym' had served its purpose and instead of coherent fixed identities, the only fixed thing was the blockchain itself. All else would be fluid, multiple, and could exist 'in the dark', shielded from the prying eyes of authorities. This intention easily and quickly flips into its opposite. Research and testing has shown several different ways that anonymity can be compromised (Meiklejohn *et al.*, 2013). A given transaction can be traced all the way to an exchange and de-anonymised at this point. Anonymity nevertheless matters to blockchain 'sensibilities' and so there are continuously new techniques and protocols being developed to improve both anonymity and privacy features (cf. Narayanan and Möser, 2017) – for example, coin mixers that 'mix' transactions so that they cannot be traced directly to specific owners. Mix nets and advanced cryptography, called zero-knowledge proofs, have also been added to the arsenal for the development of different cryptocurrencies with much stronger anonymity, like Z-Cash, Monero and more recently Nym, which have been developed specifically for anonymity purposes (Blum, Feldman and Micali, 1988; Dwork, Naor and Sahai, 2004; Saberhagen, 2013; Ben-sasson *et al.*, 2014).[96] [97] [98] Techniques like Attribute Based Credentials (ABC) selectively reveal only the minimum necessary information in order to cryptographically prove something about oneself and gain access to a system; it is a network of 'nyms' to engage freely rather than of coherent identities to be targeted. In response to those aspects of blockchain that tend towards complete determinacy, fixed identities and defined property, the fluid interactions of anonymous systems remains one of the more explicitly politically

[96] See https://z.cash/
[97] See https://www.getmonero.org/
[98] See https://nymtech.net/

aware aspects of blockchain projects and development. These are two differing tendencies in the field of blockchain that tend to either prioritise formalising and having blockchain systems adopted within existing legal, commercial and economic frameworks, or continuing its trajectory as primarily an anti-authoritarian tool.

Transparency

Transparency is, to some degree, ensured through principles of openness and trustlessness: the code of decentralised systems is open and transparent and can be reviewed, as can transaction data and the state of the Bitcoin network overall. However, there is a tension between the principles of transparency and privacy/anonymity that remains unresolved. In the Cypherpunk subculture the general ideal of transparency for the powerful and privacy for the powerless (Hughes, 1993; Assange *et al.*, 2012) was adopted, but this distinction between powerful and powerless beyond references to governments and corporations becomes less clear as when decentralisation becomes a generalised idea. In relation to specific and well understood authorities, the formula makes sense, but in terms of the Bitcoin network as a proposition in its own right, it remains unresolved because there are as of yet no agreed-upon methods to name 'the powerful' from 'powerless' in what are supposed to be decentralised systems. For example, are people with large holdings of bitcoin the 'powerful' and should they therefore have some form of transparency and accountability structures put in place? For those looking to establish accountability methods for the emerging 'authorities' amongst and within blockchain systems, I would like to suggest that although politically and ethically unresolved, the aim of systems having transparency properties can be leveraged. Indeed, the culture of anti-authoritarianism and leaking can provide a context for developing more refined accountability structures.

Capacity (scalability, speed, throughput)

Less explicitly ideological but an important property for most blockchain systems has been the question of sufficient capacity, including scale, understood in terms of volume, speed and the throughput that a network can manage. Chapter 6 discusses how a seemingly neutral technical issue such as capacity, scale and speed of a system can become hugely politicised and debated. Capacity of the network can serve different purposes and be mediated in different ways. (Bitcoin itself came out of network engineering research that sought to use price mechanisms to throttle networks in order to reduce spam and waste of network resources (Dwork and Naor, 1992; Back, 2002)). Capacity at different layers and for different purposes is therefore a fine-grained design question that tends to benefit certain types of uses over others, rather than being an absolute measure. It is nevertheless an important property in

protocol designs and the basis for many forks and new protocols looking to improve on Bitcoin. Capacity is addressed, for example, on the basis of being able to compete with existing digital payment systems, but also from a network security standpoint of achieving large enough networks for decentralisation to function effectively as a security property.

Autonomy

There is an underlying tension in blockchain systems designs between questions of autonomy as 'automation' and systems beyond control, or in the sense of self-determination and indeed bringing more control back to people using a given system. The provenance of early peer-to-peer strategies of decentralisation brought with it a very particular understanding of autonomy. Early peer-to-peer systems were built with the intention of making their shutdown impossible by ensuring that the network was not controlled by any single node, server or person, but instead run in a decentralised manner. Such ambitions understand the construction of a system that is autonomous from control to be the basis of a form of political autonomy for those that use it. As these ideas became generalised, this evolved into a particular understanding of the system itself as autonomous from human control more generally, with the aim of ensuring that various functions would execute automatically and regardless of human will or influence (see Chapter 4). Autonomy came to mean a form of automation in systems design rather than necessarily self-determination in the political sense, while the concept still maintained the social and political insinuations of empowerment in relation to authority.

These principles and properties are intended to serve particular purposes and to have certain effects. I consider such effects to be hopes and claims about what blockchain systems do, but that again should not be understood as guaranteed by the technical architecture alone.

Disintermediation

Disintermediation refers to the idea of getting rid of any 'trusted third party'. This might be in terms of the network, to disintermediate and establish a peer-to-peer network such that there are no intermediating servers, or commercial or institutional service providers more generally. Peer-to-peer systems are, technically speaking, characterised by peers in the network communicating directly with each other. Contrasted with a server-to-client model, where servers hold and serve content to various clients, in peer-to-peer networks there is no such distinction. The concept also tends to be understood in a more broad sense of cutting out the middleman (Filippi, 2013), at times as a critique of *rentier* behaviour where intermediaries are understood as unnecessary and adding extra cost (Nakamoto, 2008), at other times

referring to the security concerns from earlier years of decentralisation networks, whereby an intermediary might distort, manipulate or block flows of information, either of their own volition or due to pressure from external authorities. As discussed in more refined technical detail by Troncoso *et al.*, 2017, peer-to-peer systems can evolve into 'super-node' types, where peers with more capacity become the main relay nodes. And so in Bitcoin, there has been significant specialisation in the network over time (see 4.1.3 and 6.1.2) that arguably begins to resemble new forms of intermediation.

(Net) neutrality

One of the main intentions of decentralised architectures is that they provide a neutral network that does not 'care' who, or for what, it is used. Because the infrastructure is run by multiple nodes, even if one node is run by a person, company or organisation that might disagree with a given use, they will be unable to stop it because the message will be relayed and transaction will be processed by other nodes. Net neutrality became politicised as a legal and technical term through a case between the decentralised file-sharing system BitTorrent and major US internet service provider (ISP) Comcast. The company had been throttling network traffic when users of their services attempted to share whole files with each other (Svensson, 2007; Daniel, 2008; Smith, 2010).[99] A court ruling went in favour of BitTorrent and the concept of net neutrality: that a network should treat users equally regardless of their uses. The notion is also used as an argument for network service providers to not be liable for potential illegal uses of their services. This idea of neutrality is at times conflated with ideas of technological neutrality more generally, whereby a given technical system is thought to be neutral in terms of its effects in contrast with human-based institutions, for example when Bitcoin developer Corallo states: *'if you have a system that is much more decentralised and technology-based it is much easier to build something where you can't necessarily apply the same pressure without going all the way to making something completely illegal. You can't block these things.'* The necessary and inevitable differences of contexts, people and places, however, means that any given system will effect people in very different ways, and such an approach to ideas of power, networks and neutrality were to be complicated in disputes internally in Bitcoin and Ethereum not long after.[100]

Freedom

[99] Net neutrality is also a cultural rallying call for open network infrastructures and peer-to-peer economies, see for example this album on Napster: https://us.napster.com/artist/various-artists/album/rock-the-net-musicians-for-network-neutrality/track/red

[100] See Bitcoin developer, Matt Corallo, interviewed by iamsatoshi, Tomer Kantor, Apr 2015 https://youtu.be/0ve8hqfeM0E

Economic and political freedom is one of the major intended effects of Bitcoin and blockchain systems more generally. Bitcoin critic Golumbia picks up on the frequent mention of 'liberty' versus the 'tyranny' of governments and state violence as indication of right-wing ideology at work in Bitcoin (Golumbia, 2016). These intersect easily with right-wing and cyberlibertarian ideas, but also with ambitions of disrupting monopolies of international monetary and payment systems more generally. Bitcoin and cryptocurrencies contributed to an awareness of and debates around dependencies and geo-political dynamics in money systems. The imagined use-cases of Bitcoin and many cryptocurrency systems are therefore to circumvent financial blockades, sanctions and other legal controls to value flows. So while, for example, the short-serving Greek finance minister Varoufakis criticised the economic ideas and gold standard implied in Bitcoin, he nevertheless also suggested the possibility of a cryptocurrency that would alleviate liquidity problems in Greece due to the problem of public debt in the context of the financial crisis (Varoufakis, 2014). The ability to control money supply and circulation is considered an important aspect of being independent from 'authorities' and establishing autonomy in the sense of self-determination – and is indeed one of the intended effects of Bitcoin and many of the cryptocurrencies, alt-coins and social currency projects that it gave rise to.

Cost efficiency

In theory, because a decentralised peer-to-peer system should facilitate transactions without any intermediary, it should be more cost effective than existing payment services and infrastructures. This is one of the main arguments in the Bitcoin whitepaper for disintermediation. Bitcoin was therefore envisioned as a potential remittance infrastructure where people could freely send money circumventing both government and corporate intermediation. One of the intended effects of Bitcoin and many blockchain systems are therefore to outcompete existing systems by being more cost-efficient. Cost efficiency is in no way guaranteed by decentralised network design but is a more complex economic question that also relates to how the infrastructure is intended to sustain itself, who should get paid, for what, and how much can be charged from those using the system (see 5.2.2).

The political sensibilities of and in Bitcoin and blockchain assemblages are still very much in formation. The affiliation tends to be primarily to computational concepts, while political and economic ideas are often drawn on in an experimental manner as and when they speak to such network concerns. My attempt with the above has been to articulate some of these particular sensibilities. The common ground, and what tends to matter in blockchain, draws on ideas, experiences and approaches from network computation in relation to 'authority'. They are grounded neither in a critique nor in a total support of existing capitalist systems. In

addition, as Golumbia and others point out, there tends to be a critique of the state and government regulation, but indeed also corporate authority, monopolies and state-backed violence more generally that intersect with political interests beyond US right-wing libertarian context looking towards disrupting network monopolies. This is not trivial but suggests a form of disruption, which will be explored further in the second half of the chapter. First, however, I will trace through how these ideas and concepts became popularised beyond the immediate Cypherpunk, hacker and network cultures and took on a broader meaning.

5.1.3 From disruption to redistributing the sensible

The main concerns of decentralised peer-to-peer systems has been to eliminate the possibility of control by authorities and prevent any single point of failure in such a way to ensure that the system is reliable, resilient and can survive attacks by what engineers have called 'formidable adversaries' (Troncoso *et al.*, 2017), referring to governments, legal systems, secret services or corporate adversaries. This particular strategy was to eventually become a generalised proposition for getting rid of human intermediaries overall as these might in turn be corrupted (as discussed more below as well as in Chapter 4); it turned from an intention to defeat 'formidable adversaries' to assuming any kind of adversary. This, I argue, is in part due to the timing of Bitcoin, published and built in the midst of the financial crisis, and its testing against such formidable adversaries in the Wikileaks banking blockade. I here discuss both of these events.

Financial and political crises

The Bitcoin whitepaper was published and circulated on 'The Cryptography Mailing List' in October 2008 and the first Bitcoin transaction took place on the 3rd of January 2009, famously including a headline from that day's Times newspaper: 'The Times 03/Jan/2009 Chancellor on brink of second bailout for banks' (Champagne, 2014).[101] [102] [103] This has been interpreted as both a 'timestamp', proving the date of the transaction, and also as a means to position the purpose of Bitcoin as a critique of the existing banking system and the political handling of the financial crisis. Only a year later, another major event — the Wikileaks financial embargo — put the idea of Bitcoin and decentralised networks as a strategy against authority to a practical and very public test. The attention for and interest in Bitcoin has been traced to the timing in relation to the financial crisis, the Wikileaks case shortly after and an early article in Forbes that described a rapid increase in the value of bitcoin against the dollar (Roio, 2013). These events have become part of an established narrative of the history of Bitcoin and

[101] See https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h
[102] See https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html
[103] See https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

blockchain (Roio, 2013; Champagne, 2014). It is nevertheless worth describing them once again, focusing on how these events attracted people with several different understandings of finance, monetary theory and economics to Bitcoin, and the ways in which 'decentralisation' accommodates for these, drawing forth a sensibility along different lines.

Bitcoin's launch just as the financial crisis erupted attracted people with differing critiques of the political handing of the crisis and the financial and economic systems that gave rise to it. For theorist and blockchain critic Golumbia, the timing of the financial crisis would attract people to Bitcoin who, regardless of its usefulness as digital money, would find in and through the protocol a decidedly right-wing economic explanation for why things had gone wrong. '*Bitcoin absolutely does something, yet it does not do what many of its advocates claim it does. Bitcoin is a technology whose social and political functions far outstrip its technical ones'* (Golumbia, 2015, p. 119). He traces the provenance of aspects of the Bitcoin protocol, in particular analogies to gold mining, and fixed money supply in right-wing economic ideas and central bank conspiracy thinking from the US in particular (Golumbia, 2015, p. 123). In these theories, tyrannical governments control the printing of money and use this power to steal from ordinary people by causing inflation. The algorithmically-determined money creation and fixed money supply in Bitcoin would be an effective antidote to central bank tyranny, quantitative easing and corrupt bailouts.

Several other authors have read a commodity theory of money in Bitcoin gold analogies, also often associated with aspects of right-wing economics (Scott, 2014, 2018; Varoufakis, 2014; Golumbia, 2015). Yet it is telling that in the list of references at the end of the Bitcoin whitepaper, there is not a single reference to monetary or economic theories (Nakamoto, 2008, p. 9). Instead, the references are to cryptographic and computer engineering work. Grounding the project in computation rather than political or economic affiliations meant that Bitcoin attracted people with varying ideas and understandings of money, finance and economics, but generally with a sense that the existing system was not working. The relatively undefined monetary approach and the context of the financial crisis has indeed allowed the project to become a strong vehicle for political and economic conspiracy theory explanations from the right wing, as noted in particular by Golumbia and Greenfield (Golumbia, 2016; Greenfield, 2017). It is important to acknowledge such ideological workings of Bitcoin, but without an appreciation of the specific history and affiliation to peer-to-peer computation, many of the political ideas that inform decisions and hold together the blockchain community will be missed.

Money creation in Bitcoin takes place through what is called bitcoin mining (explained and discussed in detail in 4.1.1). The Bitcoin whitepaper states: *'The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to*

circulation. In our case, it is CPU time and electricity that is expended.' (Nakamoto, 2008, p. 4) This explicit gold analogy suggests an affiliation with or assumption of commodity theories of money: that the value of a bitcoin token is derived from the effort that is needed to create it (or, more precisely, the burning of energy while repeatedly running hashing algorithms). The economic ideas contained in the gold analogy sound convincing from a peer-to-peer perspective; money that has an intrinsic value is, in a sense, disintermediated money because it seems like it does not require an authority to back up and enforce its value. The understanding of those that, knowingly or unknowingly, subscribe to commodity theories of money is that the current value setting is determined through central bank authorities, and that instead of relying on authorities to establish and enforce the value of money should be derived directly from some intrinsic nature of the material itself, in most cases gold (Scott, 2014). Commodity theories of money relate to a longer lineage of thinking that takes markets and trade as natural rather than state enforced, and money as the most effective means to facilitate such activities. The assumption is that such intrinsic value ensures stability whereby the value is derived from the quality of the thing itself rather than enforced and determined by a government and central bank. Golumbia's work is aimed primarily at drawing out the contradictions of these ideas, pointing to the volatility of the price of gold as well as Bitcoin in the absence of any policy or regulation, and counters that the role of central banks and interest rate policies exactly serves to ensure stability; in other words, that grounding an economics and monetary approach on a notion of natural state of value, determined through the scarcity of a precious metal, is to ignore the evidence of the effects of such monetary and economic thinking that contradict the very hopes and claims. But Bitcoin did not exclusively appeal to the US right wing or those subscribing to right-wing political economy, and the Bitcoin architecture also points to a different set of monetary ideas and possibilities, one of which is an understanding of money as expressing relationships rather than an intrinsic value, namely credit theories of money (Innes, 1914).

In Bitcoin there are no self-contained 'coins' as such. Instead the system functions as a ledger of transactions and balances of accounts. It is frequently thought of as a decentralised ledger, has even given rise to so-called DLT (Walport, 2016), distributed ledger technology, a decentralised ledger of credits, debts (and witnesses, so-called triple entry accounting, (Grigg, 2005, see 4.1.1). Credit theories of money define money as credit notes that can be redeemed for some good or service. Whether expressed through tokens or ledgers, these are simply ways of making visible and registering relationships of credit and debt. The financial crisis had also spurred a different critique of money creation that focused on debt relationships and fractional reserve banking. Central banks generally do not 'print' money directly, but regulate money supply through interest rates. Fractional reserve banking allows private banks to lend amounts backed only by a fraction of the total lending. This in effect means that money creation takes place through by private banks issuing debt, and central

banks regulate by setting interest rates. This formed much of the critique of the existing financial and banking system from the political left so to speak, and here too, Bitcoin was an attractive prospect, in particular as a technology that promised the possibility of programmable money. Alternative and complementary currencies have been around for a long time, but Bitcoin introduced the possibility of deploying, securing and running alternative currencies at scale, and program more complex interoperability between these, allowing for experimentation with all kinds of economic and monetary ideas. There is therefore an important part of the history of Bitcoin, colloquially known as the time of the 'alt-coins', where the invention of Bitcoin spurred playful experimentation with lots of different economic and monetary ideas, often quite specific to different subcultures, and often driven by curiosity and humour.[104] This was a vision of decentralisation as multiple monetary ecosystems at different scales, with a focus on diversity and interoperability (cf. Bauwens, 2014; Prieto and Duran, 2015; Roio and Sachy, 2015; Pazaitis, Kostakis and Bauwens, 2017; Haiven, 2018; Scott, 2018).

The possibility of disrupting existing monetary, economic and financial systems with self-issued and programmable money along with the scope for economic experimentation attracted a more motley bunch of people to Bitcoin, cryptocurrencies and blockchain than is often appreciated. In the process, economic and political ideas were drawn on, sporadically relating to different aspects of the Bitcoin architecture and its history in decentralised network technology. Decentralisation was a strategy used to circumvent pressures or control by authorities and prevent forced shutdown. 'Authority' in turn came to also mean any node internally in the network that would need to be trusted in order for the system to work as intended. If any aspect of the system would have to be fully trusted then this could become a target for governments or corporations looking to close down the system. For network security reasons, the ideal was to approach trustlessness. With the financial crisis the question of trust took on a broader meaning, and indeed the ideal use-case continues to be resilience towards untrustworthy authorities in conditions of economic tensions, from Greece (cf. Varoufakis, 2014; Richards, 2015), to India (cf. Higgins, 2017) and Venezuela (cf. Bambrough, 2018; Chandler, 2018; Crypterium, 2018; Voge, 2018) – in ways that have also been critiqued as a form of technology-driven colonialism (Scott, 2016). In the financial crisis, economic and political authorities showed themselves to be untrustworthy, a context that lent a much broader political-economic dimension to the concept of trust and many other concepts in decentralised network computation. An architecture that promised 'trustlessness' went from being a particular notion in network computation to an enticing narrative for political, economic and social systems more broadly.

[104] See https://dogecoin.com/ for one of the more long-standing alt-coins with a dedicated following. Some years later, when conflicts broke out as to the development pathways of Bitcoin, the term alt-coin started to be used in a derogatory manner. Different versions of the Bitcoin protocol were being created, some of which were called alt-coins as a way to state that they were not the 'real' Bitcoin.

Wikileaks banking blockade

> So for example if you have PayPal; it is very easy to apply pressure on PayPal to make significant business decisions, for example to block Wikileaks, without necessarily applying a law and going straight to PayPal and say we are going to sue you, right? Whereas if you have a system like Bitcoin or if you have a system that is much more decentralised and technology-based it is much easier to build something where you can't necessarily apply the same pressure without going all the way to making something completely illegal. You can't block these things.
>
> – Bitcoin developer, Matt Corallo, Apr 2015[105]

In 2010, the ability of decentralised systems to withstand attacks and be censorship-resistant was put to a very public test. The whistle-blower website Wikileaks faced an unofficial banking blockade, meaning they could no longer receive donations. What emerged out of the Wikileaks situation was a political justification for Bitcoin as a peer-to-peer money system in relation to existing political and economic systems. For many, what was revealed in this moment was more than repression of Wikileaks; it showed that the financial system, and indeed the internet itself as it had developed, were far from a free and neutral global infrastructure, and that the US had a very real *'kill switch to any organisation anywhere in the world'* through their control of the handful of companies that facilitated nearly all of global value flows.[106] And so the events attracted the attention of many for whom infrastructures and networks are supposed to be neutral and facilitate free exchange of value and information and who were outraged at their control and manipulation for geo-political purposes.

The founder of Wikileaks, Julian Assange, was involved in the Cypherpunk movement, a political subculture that came about in relation to concerns of privacy and transparency in the face of power. Cypherpunk grew out of parts of peer-to-peer culture and the capacity of cryptography to modulate questions of privacy and transparency in such ways as to be unbreakable by even the most powerful actors (Hughes, 1993; Assange *et al.*, 2012). The vision was to enforce transparency on the activities of the powerful, through whistleblowing and otherwise, while protecting the privacy of the powerless through for example private key encryption technologies. The work of the whistle-blower website in exposing government corruption and violence, and involvement of Assange with Cypherpunk movement, resonated with the intentions of Bitcoin as a means to establish a network of value flows beyond the control of authorities. So when Wikileaks came up against a banking blockade, a perfect use-case for Bitcoin started to emerge. The first mention of potentially helping the organisation

[105] See https://youtu.be/0ve8hqfeM0E
[106] Quote from Rick Falkvinge, founder of the Pirate Party in Sweden, in an interview in the documentary Ulterior States https://youtu.be/yQGQXy0RIIo?t=11m42s

was posted on *bitcointalk*, the main forum for the Bitcoin community in 2010 when the project was still very small and mostly unknown:

> Hey,
> I wanted to send a letter to Wikileaks about Bitcoin since unfortunately they've had several incidents where their funds have been seized in the past.
>
> Anyone know where to send a message to them?
>
> – genjix, November 10 2010, 12:49:16 PM[107]

While for some in the Bitcoin community this was an exciting opportunity to test the security and capacity of the project and support an ally, for others, this would attract attention too early and potentially destroy the project, and so a longer discussion ensued on the forum.[108] But the news began to circulate about the latest leaks, the US military war logs by US army soldier Manning with evidence of the killing of civilians in Iraq and Afghanistan, including very explicit video recordings of drone strikes. Shortly after, with no court order, Paypal, closely followed by most major international money transfer companies, blocked donations to the organisation.[109]

> Paypal just blocked them, and they're trying to get other US banks do the same. This would be a great moment to open bitcoin donations.
>
> – wumpus, December 04, 2010, 08:47:59 AM[110]

There were strong disagreements in early discussions on the *Bitcointalk* forum about whether Bitcoin should publicly support Wikileaks, and thereby become an explicit strategy for circumventing authority, or aim for everyday adoption for regular payments. In particular, there was hesitation about how such a politicised act might affect Bitcoin companies and exchanges. Bitcoin, as a proposal for a peer-to-peer money system, had brought together a wide-ranging set of people attracted to the capacity that peer-to-peer networks have in circumventing controls of money systems. But there were diverging opinions as to what extent the purpose was to circumvent and resist political control of such a contentious and high profile kind as in the Wikileaks case, or whether the project would be better off operating and expanding in more mundane contexts: *'I say, we MUST get Bitcoin accepted at Starbucks*

[107] See https://bitcointalk.org/index.php?topic=1735.msg21271#msg21271
[108] See the full chat log archived here: http://archive.li/Gvonb
[109] See for example https://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin/#4bb337b77202 and http://www.coindesk.com/assange-bitcoin-wikileaks-helped-keep-alive/ and https://www.reddit.com/r/Bitcoin/comments/5ai3x1/fact_wikileaks_the_whistleblowing_website_turned/
[110] See https://bitcointalk.org/index.php?topic=1735.msg26737#msg26737

and the local grocery store.... BEFORE it gets accepted at Wikileaks.' Some were worried that political association with the organisation would kill the project from its infancy: *'Currently all intelligence services are working to smash wikileaks. I would not want to suddenly posthumously come into Al-Qaeda.'*[111] Others argued that this was the moment to prove the efficacy and necessity of a system like Bitcoin: '*PayPal just blocked them, and they're trying to get other US banks do the same. This would be a great moment to open bitcoin donations*' and '*bring it on. Let's encourage Wikileaks to use bitcoins and I'm willing to face any risk or fallout from that act.*' The inventor/s Satoshi Nakamoto disagreed: *'No, don't 'bring it on'. The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage.'* A few days later, on the 10th of December, an article was published on the PCWorld website suggesting the Wikileaks situation was giving rise to renewed efforts of blocking censorship through peer-to-peer networks, and discussing and introducing Bitcoin as the latest in that field. This public connection, between Wikileaks and Bitcoin had this response from Nakamoto:

> It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us.
>
> – satoshi, December 11, 2010, 11:39:16 PM[112]

After this post Satoshi Nakamoto largely disappeared from forums and discussions. (According to Wikileaks founder Assange, the two of them had agreed that it was too early to use Bitcoin, and so it was not until six months later on 14th of June 2011 that Wikileaks created and published an address to receive donations.)[113] [114] In some ways these types of disagreements continue to this day, between those seeking to develop Bitcoin as a legitimate and broadly accepted means of payment, and those who understand the project as primarily a strategy against authorities, whether for very specific geo-political purposes or as a general attitude and a means to maintain a network beyond the reach of authorities. The voice of the absent authority of Satoshi Nakamoto has often been conjured to support development pathways towards everyday payment systems (see, for example, Bitcoin Cash), but the open decentralised characteristic of the project does not easily conform to authorities, whether the authority in question is the supposed inventors or not.

---

[111] See bitcoinex https://bitcointalk.org/index.php?topic=1735.msg25360#msg25360
[112] See https://bitcointalk.org/index.php?topic=2216.msg29280#msg29280
[113] https://www.reddit.com/r/Bitcoin/comments/5ai3x1/fact_wikileaks_the_whistleblowing_website_turned/ and https://www.coindesk.com/assange-bitcoin-wikileaks-helped-keep-alive.
[114] See https://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/#4f21fee54f73 and https://www.blocktrail.com/BTC/address/1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v and https://news.ycombinator.com/item?id=15480644 and https://www.wired.com/2010/12/paypal-wikileaks/
Wikileaks donations page: https://shop.wikileaks.org/donate

The Wikileaks case has been described as a determining moment for Bitcoin (cf. Roio, 2013; Grigg, 2016), going from an obscure experiment to emerging and proving itself, practically, as a global value-network capable of evading and circumventing controls by authorities. Such a possibility embodied the ideal of a global platform for the circulation of value that would be neutral because it was technologically beyond the reach of authorities, thereby contributing to the possibility of political contestation. It was not just that Bitcoin provided an alternative means of value transfer – its very architecture, the fact that it was decentralised and could therefore not be shut down by anyone, came to represent a solution to centralised power. This, in turn, was related to another notion that had come out of peer-to-peer forming part of a blockchain sensibility, namely net neutrality. In the earlier history of legal cases around breach of copyright taking place in file-sharing networks, the argument was that those providing infrastructure should not and could not be prosecuted for breach of copyright taking place on these networks. They were providing an infrastructure that was accessible to anyone, but could not be held accountable for what took place on it. Internet providers, in contrast, were perceived by peer-to-peer communities as threatening net neutrality, by blocking or throttling different kinds of content, on the basis of legal pressure by IP holders as well as political or religiously motivated forms of censorship – related to debates around free speech that are alive to this date. Through the Wikileaks case, the control of global flows of value became in many peer-to-peer communities linked to free speech, and ideas of freedom more generally. 'It is much more about how can people exchange different forms of value as free speech', said early Bitcoin entrepreneur Elizabeth Starks.[115] These ideas of net neutrality, through the Wikileaks case, became justified at a geo-political scale, related to US control of international value transfer networks. To this date, a commonly mentioned and pursued use-case of Bitcoin is for circumvention of financial embargoes and control and the establishment of net neutrality in the sphere of international value transfers, including examples like Iran, Kurdistan, Ecuador, but also Russia and Chinese interests in the relationship between the control of network infrastructures and geo-politics.

The intention with the first half of this chapter has been to give some context and understanding for how the particular operationalisation of concepts in peer-to-peer computation and network political cultures would come to resonate with broader political events in such a manner as to take on meaning beyond their immediate strategic applications to become a sensibility and proposition in its own right. While certain operationalisation of ideas of decentralisation indeed relate to US right-wing economic and monetary ideas, there are histories and reasons for why Bitcoin did not exclusively attract the political right and instead presents a broader political scope than that, based on ideas that are derived from network computation and the capacities of these to be used as a means to circumvent

[115] Elizabeth Starks, Interviewed by Tomer Kantor iamsatoshi, April 3rd, 2015, https://youtu.be/B3K5aVvqt7U [accessed 16.11.2018]

authorities. There are considerable political differences and differing economic ideas circulating in and amongst blockchain projects and yet there is also an assemblage, a common sensibility that holds the community together despite the differing economic, social and political backgrounds.

The attraction of Bitcoin and decentralised technologies was the possibility of circumventing authorities. However, since the invention of Bitcoin and the increasing attention of blockchain, a critical body of literature has appeared, raising concerns about the ways in which blockchain systems might instead lead to *increasing* authoritarian control (Scott, 2014; Herian, 2016; Käll, 2018; Manski and Manski, 2018). How did this transformation take place, and what kind of authorities are emerging in and through blockchain? In the following section, and with the invention and launch of Ethereum, I discuss how what I have described as blockchain 'sensibilities' became generalised in much more explicit ways. The provenance of early peer-to-peer understandings and operationalisation of decentralisation and a particular form of network anti-authoritarianism would have significant and in some ways contradictory effects on the social, political and economic purpose and imagined use-cases of blockchain technology more generally.

5.2 Decentralisation generalised

Ethereum marked a shift from decentralised systems that were application-specific to generalised protocols and platforms. The project sought to take the Bitcoin architecture and make it Turing-complete, meaning able to run any kind of computation. Instead of a decentralised system for verifying and storing transactions, Ethereum would be a decentralised system for storing and running any piece of code. This chapter has so far traced concepts and ideas that form a blockchain sensibility through a pre-Bitcoin history in order to understand its provenance as a strategy for circumventing authority and in the thinking and reasoning of network security under conditions of decentralisation. In the following, I argue that the Ethereum blockchain project makes explicit two major changes to previous generations of decentralised network projects since Bitcoin, namely the *generalisation* of these concepts and ideas, from particular strategies in the face of 'formidable adversaries' into general platforms resulting in systems designs in and for themselves, and the incorporation of economic dynamics into protocol design through *tokenisation*, opening up a new field of cryptoeconomics and shifting the political economic assumptions in network culture. The ideas informing this understanding of decentralisation form a particular sensibility that does suggest a kind of 'disruption', but does not follow along the lines of explicit critiques of capitalism, nor necessarily 'the state' in the case of Ethereum,

but rather ideas of decentralisation, trust, authority and autonomy as articulated above. And so many aspects of market and state techniques are indeed reproduced and in some ways strengthened and extended through Ethereum, while it nevertheless poses challenges to existing state, financial and commercial business models. The extent to which such a disruption and sensibility has been articulated clearly and is enough of a priority to enable a 'redistribution of the sensible' remains to be seen and is still very much up for negotiation.

In the second half of this chapter then, I here discuss the ways in which decentralised protocol design was first 'platformised' in Ethereum. As a platform Ethereum was intended as a disruption to existing platform monopolies, but could be argued to present an emerging kind of platform monopoly in its own right – this time on a protocol rather than application layer. As such, and with the incorporation of market dynamics into several aspects of the protocol, the project could easily be read as another frontier of platform capitalism (Langley and Leyshon, 2016; Scholz, 2016). This contradiction is resolved from the perspective of Ethereum through notions of zero-trust systems, namely that the platform should not be perceived as another trusted intermediary exactly because it is trustless. This notion in the meantime point towards significant governance questions on the protocol level. If the platform is intended to be neutral with no trusted intermediation, then how the code is written and run, who gets to decide on changes to the protocol and how become the main site of differentation (discussed in detail in chapter 6). Here, I draw on a diverse economies approach (Gibson-Graham, 2008), this time not necessarily to look for diverse economic dynamics but rather to shift the attention to the multiple possibilities at play in relationships with existing systems. I argue that much of the meaning of Ethereum, and indeed most blockchain systems, comes from their articulation in terms of such relations. I argue that the project of generalising the principles of the Bitcoin protocol removed these from their articulation and meaning in relation to specific authorities, and in the process lost much of their reasoning. 'Decentralisation' became a vague idea in and for itself but without much clear definition or purpose, systems and protocols being addressed as hermetic systems on the basis of whether or not they fulfilled abstract notions of decentralisation rather than a particular purpose in relation to the context of their use.

I argue that bringing into play some of the initial motivations for decentralisation clarifies the particular disruptive potential of the technology – for example, the potential to platformise the design of decentralised systems that would make advanced cryptography more accessible. This ambition is indeed one of the main ones in the Ethereum project, namely to radically transform the underlying internet protocol such that existing surveillance-based business models are made technically and economically unfeasible. From this point of view, the incorporation of economic dynamics into protocol designs might be read less as a straightforward advancement of capitalist market logics, and more as a politicised project to

outcompete current internet business models by attempting to make surveillance-resistant protocols economically viable and attractive.

The generalisation of Bitcoin systems design principles also brought with it a second major change to decentralised protocols, namely tokenisation. Tokens suggest the possibility of a system that pays for itself by incorporating an internal economy. I discuss this hope of a systems design that pays for itself, again drawing on Gibson-Graham (2018), but this time to suggest a shift in attention when looking internally in the protocol designs to address relationships with existing economic dynamics. I analyse the tokenisation of protocol designs, discussing first the emerging field of cryptoeconomics, suggesting that here too, the relationships with existing economic spaces is what matters the most – incorporating a token into a protocol does not make that protocol economically autonomous; rather, it draws in all manner of economic dynamics into the protocol itself, starting from exchange rates. Finally, I discuss the ways in which tokenisation has shifted the political economic assumptions in network culture, from one founded on openness and a critique of in particular intellectual property, to one of multiplying propertied relationships and their immediate enforcement. While this is no accident, given that cryptography indeed is a technology for determining access, I argue that it is not an inevitable outcome. By drawing on the earlier histories of decentralised systems designs, a blockchain sensibility does lend itself to more critical ideas of property and access, but that such an agenda would require consistent theoretical and practical effort.

5.2.1 Platformising decentralisation

In the first formal public presentation at the 2014 North American Bitcoin Conference in Miami, Florida the then 20-year-old founder of Ethereum, Vitalik Buterin, reframed the core contribution of Bitcoin from a peer-to-peer currency to a 'global trust-free decentralised database'.[116] Bitcoin had spurred a whole variety of monetary experimentation in new 'alt-coin' cryptocurrency projects, but it had also brought ideas of how this architecture might support long-standing ambitions towards decentralisation in other aspects of the architecture of the internet, including for example website domain name registration.[117] In the launch of Ethereum, these developments were narrated into a more explicit history. Until then, Bitcoin had been a proposition for decentralised digital money. The Ethereum whitepaper articulates a lineage, tracing the development of 'trustlessness' from pre-Bitcoin experiments with online currencies (Chaum, 1998; Back, 2002; Grigg, 2014), through Bitcoin to Ethereum.[118] [119]

[116] See the full presentation here: https://youtu.be/I9dpjN3Mwps Buterin initially announced the project on Bitcointalk.org (https://bitcointalk.org/index.php?topic=428589.0) in 2013 just a few months before formally presenting it in Miami.
[117] See https://www.namecoin.org/
[118] See https://github.com/ethereum/wiki/wiki/White-Paper, accessed 29th May 2017

Bitcoin had shown how decentralised consensus could be organised in a 'trustless' manner, and the Ethereum project would build on that advancement in order to generalise decentralisation. The particular understanding of decentralisation that is sought to be generalised is completely in coherence with its history as network design strategy, with the associated network security ideas of trustlessness. In the first public presentation of Ethereum, Buterin thereby articulated what was to become a common explainer in efforts to make Bitcoin palatable beyond the reputation as a means of payment for illegal activities; namely that the ground-breaking contribution of Bitcoin was not so much decentralised money but the decentralised database and consensus process – in other words, the 'blockchain', and the proof-of-work consensus protocol. Ethereum was to expand the capability of this design into a 'featureless layer' on top of which any type of application might be built (Ethereum, 2014; Szabo, 2014; Wood, 2014a; Buterin, 2015) what people were starting to describe as 'next generation' blockchain to signify the shift from application specific designs to generalised protocols.

In Buterin's first presentation he suggested three potential uses of the Ethereum project's generalised protocol, namely so-called Smart Contracts, Decentralised Autonomous Organisations, and Web 3.0. The reasoning and motivation for these can be traced directly from the political sensibilities of early decentralised technologies, into a more generalised form. Previous generations of decentralised projects therefore explain much of the thinking behind and reasons why these particular applications are considered desirable. Firstly, Smart Contracts are essentially bits of code that are deployed on the blockchain, stored and run across a decentralised network. Running code in this manner is hugely ineffective in terms of speed and resources, but the primary aim is that the code is held and run in a decentralised manner that cannot be shut down or stopped by any authority. In other words, just as the file-sharing network BitTorrent had been developed in order to make it impossible to shut down by authorities, Smart Contracts are equally deployed with the intention to make it impossible for any authority to stop them. They are 'Smart' because their execution is somewhat automated by economically incentivising others in a network to run them, and that the network is decentralised enough for it to be beyond control or shutdown by any single person or authority (see 4.2.1). This anti-authoritarian motivation and pre-history is glossed over by the generalising the problem of trust from specific institutions and governments to anything that could possibly be understood as currently operating in a centralised manner. Smart Contracts were not marketed as a technology to circumvent authority, but as being beyond the control of potentially anyone, and addressing a more general question of trust and trustlessness. They came to represent the possibility of automating aspects of contract law and business management rather than a direct challenge to specific authorities.

[119] As well as **forks** of Bitcoin like Litecoin and additional functionality on top of the protocol, like Namecoin, Coloured Coins and Metacoins.

Similarly, in what are called Decentralised Autonomous Organisations (DAO) – clusters of Smart Contracts that comprise an organisational form – here too the intention is for a DAO to run autonomously from any authority. Again, it is important to note the very particular understanding of authority and indeed autonomy operationalised here: the idea is that a DAO is 'autonomous' because it operates purely on the basis of the code it comprises rather than any human interpretation, and exists beyond the capacity for shutdown by any authority because it is on a decentralised network that is resilient to authorities. (Both claims were to be severely reconsidered in 2016 and 2017; see Chapter 6). Authority, in turn, was at the time understood as any person, organisation, or otherwise, that would be in a position to control or shut down a DAO; in other words, any human being. If a particular human would be able to shut down or modify a DAO, this would mean that person would have to be trusted and this would be a security weakness: the person might be corrupt, or a malicious government or corporation might take advantage of and pressure this person, which in turn could lead to censorship and all manner of tyranny. In order to prevent any such security weakness a DAO needs to operate beyond the capacity of any human to stop it or shut it down. By generalising trustlessness, the ability of any human to influence a given code or system would potentially be treated as a security threat (see 4.2 for a discussion of DAOs). The third use-case suggested for Ethereum was that the platform would make possible a Web 3.0, a redecentralisation of the internet such that the infrastructure would no longer be dominated and in the hands of a few monopoly companies and the associated government pressures. This use-case is discussed further below, in relation to events that were to become the political justification of Ethereum, namely the ways in which existing internet infrastructures were sustained by mass surveillance as revealed in a leak by former CIA employee Edward Snowden. The Snowden revelations, on the one hand, form a political and technical reasoning for 'zero-trust' systems and the need to generalise these to the internet more broadly, but they are also an important reminder of the particular remit of decentralised systems towards specific purposes rather than a generalisation of their particular understandings of decentralisation in and for itself. Here, I discuss the platformisation and disruptive potential of the blockchain sensibility.

Neutrality and 'zero-trust' interaction systems

> As we move into the future, we find increasing need for a zero-trust interaction system. Even pre-Snowden, we had realised that entrusting our information to arbitrary entities on the internet was fraught with danger. However, post-Snowden the argument plainly falls in the hand of those who believe that large organisations and governments routinely attempt to stretch and overstep their authority.
>
> – Gavin Wood, 2014b, Ethereum

> The Internet enabled Google, Facebook, Amazon, Apple to connect the world under their third-party custody. Blockchains can enable connecting the world under the custody of the participants.
>
> – Jon Choi, 2017, Ethereum[120]

If the financial crisis and the Wikileaks banking blockade broadened the appeal and meaning of the political sensibilities in Bitcoin, the political reference for Ethereum was the 2013 leak by former CIA employee Edward Snowden, giving evidence of mass surveillance by the National Security Agency of the United States and international surveillance collaborations, working with large telecoms companies and search engines such as Google and Yahoo. These events had pointed to the ways in which the internet, with its existing architecture, had become a tool for mass surveillance and geo-political control. Buterin, as well as co-founders Wood (2014b) and Steiner (2018) positioned Ethereum as enabling what a broader coalition of technologists were aiming for, namely a Web 3.0 to redecentralise the web.[121] The ambition of Web 3.0 is to create internet protocols that would eliminate third parties, 'authorities' that might be pressured and compromised by governments or corporations and make possible a decentralised peer-to-peer Internet. In the above quotes, two visions for how such efforts might look can be gleaned: an *'increasing need for a zero-trust system'* and that *'blockchains can enable connecting the world – under the custody of the participants.*' If decentralisation could be cryptographically and mathematically guaranteed and secured, then the problem of authority would be solved. By generalising this design for any and all applications, decentralised 'zero-trust' protocols – protocols that would not require trust in any third party – could be platformised and the problem of 'authority' solved for any type of application, protocol or system.

Ethereum has, from the start, been positioned as a significant disruption to existing internet architectures, suggesting a technology-based internet governance beyond the control of any authority based on the idea and ambition of a neutral system. However, by developing a generalised platform, Ethereum also generalised the 'problem of trust'. Similarly to 'decentralisation' this generalisation of the idea of trustless systems has caused confusion, conflating the network security concept with a more general social condition of trustlessness, lending trust instead towards notions of an algorithmic neutral mediation. This conflation of trustless systems designs with socio-political notions of trustlessness nevertheless proves productive for the Ethereum project in several ways. Most notably by addressing issues of platform monopolies, as well as the enforcement of law through the question of trust and network security de-politicises the proposition and turns the debate into a question of network security.

[120] See 10:52 https://youtu.be/6iEpqbACLbY
[121] See for example https://web3summit.com/ and https://web3.foundation/ and http://www.decentralisedweb.net/

A ‘zero-trust’ system entails a system where no single aspect needs to be trusted. It is therefore considered beyond the control of anyone and also neutral. The foundation of a philosophy of decentralisation coming out of trustless systems means that many questions that might be considered social, political, philosophical are framed as security questions or pushed to other layers that do not concern the neutral protocol. Making the issue one of centralisation versus decentralisation means that any critique of existing platform businesses, whether from a capitalist or anti-capitalist, whether to do with capitalism or *rentier* behaviour or security issues, can be incorporated with decentralisation offered as the general solution. This understanding of zero-trust systems in the meantime allows for a curious contradiction whereby protocols can aim towards monopoly status, to become the protocol on top of which all other protocols, applications or token systems are built, while still maintaining an ethos of decentralisation and anti-monopoly and anti-authoritarianism. Because the given system is supposedly beyond the control of even those who built it, it is not considered an intermediation, but a neutral protocol substrate.

There are some interesting contradictions between the ambition of becoming a generalised technology-based solution beyond control and the suggestion of an internet ‘under the custody of the participants’, or to put it differently, ‘disintermediating’ (one of the most commonly stated aims of blockchain systems) while aiming to become the sole medium through which this would take place. Ethereum was positioned as an explicit disruption to and critique of platform businesses like Uber and AirBnB (Valenzuela, 2016), disintermediating the digital economy of intermediaries. However, the platform economy itself can be traced to pre-blockchain efforts and excitement over the possibilities of peer-to-peer architectures that in turn led to new forms of intermediation and platform businesses (Scholz, 2016). The hopes for peer-to-peer technologies were that these would allow people to share knowledge and resources directly with one another. But instead of direct communication between people, what emerged were new platform businesses that facilitated such connections, becoming types of monopolies in their own right, and this led to the emergence of the so-called ‘platform economy’ or ‘platform capitalism’ (cf. Langley and Leyshon, 2016). A description of emerging platform economics offered by van Dijck (2013) defines platforms as establishing multi-sided markets, giving rise to new business models and financial products that curate connectivity. New platform business models would seek ‘rapid upscaling and extracting revenues from circulations and associated data trails’ (Langley & Leyshon, 2016, p. 2) in order to, following O’Dwyer, (2015), become monopolised *rentiers* of network data circulations. Platform businesses, instead of empowering individuals, largely created an ‘on-demand service economy’ where human labour could be plugged in as and when needed, with companies evading existing labour and tax regulations in the process (Scholz, 2016).

In each of the above mentioned senses, Ethereum is indeed a new kind of platform intermediation, but this time on a protocol layer (Buterin compared Ethereum to TCP/IP, the protocol of the internet); many blockchain projects seek 'rapid upscaling' to become the generalised platform on which all other tokens, contracts or protocols will be built, essentially seeking a form of monopoly status. They also facilitate connections and establish new multi-sided markets, providing the conditions for decentralised markets at the data layer (and not only between people but also between things with ambitions for Smart Contracts in IoT economies); these are paid for through fees that, seen in a different light, might also be considered network rent. Indeed, the general gist of Smart Contracts and their clustering into Decentralised Autonomous Organisations is exactly to approach human labour as something to be plugged in as and when necessary. Finally, in keeping with the history of decentralisation as a strategy of circumvention, blockchain projects are often unapologetically positioned as vehicles for circumventing regulation and taxation. There are two ways in which Ethereum proposes a disruption and difference from existing forms of platform intermediation: firstly through the idea of trustlessness, such that the platform would be beyond the control of even those who build and maintain it (that points to major questions of governance and protocol governance, the topic of Chapter 6), and secondly by making existing platform business models technically and economically unfeasible by addressing centralisation in terms of data ownership, storage and management, and reorienting the economic activities around these.

Figure 5. First Ethereum DevCon, Gibson Hall, City of London, 2015 (authors image).

The existing digital economy has been articulated as 'surveillance capitalism' (Zuboff, 2015) to describe the ways in which Google, Facebook, Amazon and others rely on mass data-harvesting for their business models. The Ethereum project does not suggest a disruption of nor is critical of capitalism as such, and the emergence of 'platform capitalism' is not an explicit concern of most people involved. The very first developer's conference of Ethereum was held at Gibson Hall in the City of London financial district, and the intention of the particular kind of 'disruption' marketed by Ethereum was amongst other things to outcompete existing financial services by platformising finance (quickly leading to the emergence of the so-called FinTech industry as the financial industry embraced the 'disruption', hired blockchain developers and started 'sandboxing' financial applications of blockchain). But to dismiss Ethereum as 'business as usual' would be to misunderstand, and miss out on, the particular forms of disruption proposed in this new generation of decentralised technology on the basis of a blockchain sensibility that I have been articulating throughout this chapter. Concerns for central control of various aspects of infrastructure, data and economy do open up important political differentiation and new sensibilities. In what might seem a perversion of Gibson-Graham's diverse economies, there is nevertheless diversity in and amongst capitalist modes of accumulation that can pose significant disruption in ways that are not entirely predictable, in particular because in this case the ideas that inform them are founded in network computation over and above any particular business model.

The difference between blockchain systems and existing surveillance-based internet infrastructure models is repeatedly articulated as one between 'centralisation' and 'decentralisation', but with a very specific operationalisation of these terms in mind. The distinction is neatly captured in this quote from an interview with Buterin, founder of Ethereum: *'This is the difference between people like me and Mark Zuckerberg. I live in a world where I presume that I could be a potential adversary to the system.'*[122] What Buterin is saying is that the Ethereum platform is built in such a way as to be beyond the control of any authority, including himself (a claim that could be contested, see 6.2). Claims of neutrality and zero-trust systems aside, there are two important differences to surveillance capitalist business model or platform capitalism. Firstly, for the system to be resilient towards for example Buterin as adversary, the data itself would need to be beyond his control, in this sense held in a decentralised manner. Secondly, the writing, running and maintenance of the system, namely protocol governance, would also need to be decentralised. Both of these areas present potentially significant differences and challenges to infrastructure business models based on data extraction. While there is nothing guaranteed in terms of control of data or things like privacy in the Ethereum platform itself, nevertheless a platform where data is held in a decentralised manner changes certain underlying dynamics in potentially radical

[122] Buterin, interviewed by Obrist, 2018 https://tankmagazine.com/issue-74/features/vitalik-buterin/

ways. A decentralised platform that would not economically depend on data extraction and that simplifies some aspects of advanced cryptography would indeed open up possibilities for a significantly different type of protocol level infrastructure both in terms of businessmodel, technical architecture and questions of privacy.

It is important to still keep track of the provenance of this conception of decentralisation as it points to some important details in what matters to those building Ethereum protocols. Decentralisation was a strategy for ensuring that a system would be resilient to authorities. In the meantime, the primary concern here is computational, and has to do with the survival of the system itself while very few promises that can be made for those using the systems in terms of protection from authorities, empowerment or risk more generally. This is a common misconception, as there is a tendency to conflate the interest of the system with the interests of society or people more generally. A trustless system does not mean trustless for those using it. Because any internal component of the system might be adversarial, the nature of the system is radically different from other systems. The system itself is open, meaning when determining the security of the system, it is for the system itself, but not necessarily for those involved. In the meantime, the effects of platformising decentralised architectures mean that advanced cryptography and some aspects of decentralised data storage can be made more accessible. An ideal outcome of platformising the engineering of decentralised protocols then would be to make accessible the design of privacy-aware platforms that would force a renewed consideration for what kinds of economic dynamics should and could fund internet infrastructures.

The hope: a system that pays for itself

A major attraction of Bitcoin, and the idea of incorporating tokens into a decentralised system more generally, was the idea of a system that pays for itself. Decentralised infrastructures had largely been run voluntarily or with ad-hoc funding in ways that were difficult to scale. The possibility of a system that pays for its own upkeep by incorporating an internal economy was therefore an attractive prospect. Major internet companies like Google, Amazon and Facebook had developed business models that were able to offer services for free by turning service users into the product. People's attention and behaviour would be captured, profiled, targeted and sold for advertisement. From there, it was a short jump for such profile and targeting techniques to be repurposed for security and military systems (Amoore, 2007, 2014) and led to what has been called surveillance capitalism (Zuboff, 2015). Rewarding miners to run the Bitcoin network and verify transactions opened up a broader idea that designing economic incentives and token economies into the systems could make the infrastructure economically self-sustaining such that it would not be dependent on service providers and surveillance-based business models.

Decentralised infrastructures that are run by communities with specific interests can be driven and motivated by a common vision and funded through external communities of support. The question of trust is largely understood to crop up at larger scales. For decentralised systems that aim at global scales and for general purposes there is an issue and question of motivation and accounting when running systems for the benefit of other strangers. The reasoning of tokenisation is that if decentralised protocols are to be generalised and operated across networks of people and organisations that do not know or trust one-another, these would need some other form of more universal motivation to contribute and a means through which to account for such contributions. The Bitcoin incentive structure proposed a solution to the issue by introducing a 'universal' incentive through a token economy. An infrastructure that would not rely on data extraction, but incorporate an internal economy such that people instead could contribute to and use the infrastructure on a peer-to-peer basis, was an attractive prospect. For part of the peer-to-peer community, then, the vision was to radically transform the internet ecosystem into economically sustainable infrastructures and alleviate voluntary work on the basis of ideals. The hope was a system that would pay for its own upkeep, thereby technically and economically disrupting existing internet infrastructure models at scale, and thereby making a blockchain sensibility economically viable. Token economies have in the meantime indeed created new communities that also rely on levels of trust (see in particular Chapter 6), and claims of universality and neutrality should be qualified and understood as some of the main promises and claims made in these communities.

Creating a token is not the same as an economy. And so the hope of creating a system that pays for itself does face significant economic questions. Ethereum and blockchain systems had been addressed largely as hermetic systems, and deployed with the assumption of wholesale replacement of existing systems. This meant that the ongoing interrelationships with already existing diversity of economic contexts was given only cursory attention in terms of deployment rather than protocol design. But the economic sustainability and power of Ethereum or Bitcoin or any given token-based platform is dependent on exchange rates and the full range of events and actions that might affect these, which in turn therefore also affects the level of remuneration of a miner or node, and the cost of running a Smart Contract or an application. This detail and consequence of incorporating economic dynamics into protocol design was sidelined for the first many years of blockchain development as an unfortunate side effect rather than an integral aspect of how the system plays out. The motherboards, computers, cables and energy being used in sustaining the Bitcoin network were still purchased using dollars, yen, pounds and euros etc., not to mention all the other resources and basic needs of people engaging in and developing the system. The price of bitcoin against these fiat currencies mattered and still matters significantly for the ambition of developing systems that are autonomous from existing economic spaces.

Between 2014 and 2018 the price of bitcoin fluctuated wildly with an overall tendency of substantial increase in value against the dollar. Towards the end of 2017 the price shot up reaching at one point $20,000 per bitcoin, with Ethereum and many other cryptocurrency projects following the trend. The wild fluctuations attracted news stories of Bitcoin as a Ponzi scheme and of people getting rich fast or losing a hard drive with all their bitcoin and other dramatic life changing sums of money either made or lost by individuals around the world. Whether positive or negative, the news stories seemed to attract more and more people to cryptocurrencies.

Figure 6. Chart of the market capitalisation and exchange rates of bitcoin to US dollars between June 2016 and December 2018, from https://coinmarketcap.com/currencies/bitcoin/

An emerging culture of DIY speculators and cryptocurrency trading experts developed and for some time it seemed as if the main use-case for cryptocurrencies was not exactly decentralised applications but to facilitate and make available financial speculation and currency trading to a much broader segment of society by operating in an unregulated field with few barriers to entry.[123] [124] Bitcoin had gone from an alternative to the financial system to spurring a decentralised and unregulated version of it. Such speculative behaviour is often criticised and the token economies understood as scams. It is worth acknowledging that the period of speculation functioned as a large fundraising drive and was experienced as empowering (see @coin_artist tweet below). For some, here was a potential to 'democratise finance', and a community that was accumulating attention, wealth and power at a very fast

[123] See for example https://twitter.com/Crypto_God
[124] Apart from familiarity with the system – for which a substantial amount of effort went towards making knowledge of these new complex systems more accessible and readily available.

pace, while for others, this was a period rife with scams and Ponzi schemes.[125] The tweets below are examples of the kinds circulating at the time, and both point towards Bitcoin experienced as an empowering technology, and yet both also entail an unsaid dependency on the exchange rate at the time – for @coin_artist in the way that her bitcoin made her suddenly very wealthy, and for Kevin Pham by moving wealth from the Venezuelan peso to bitcoin as a means to avoid the rapid inflation that was happening in the country at the time. Both tweets took place as bitcoin had been rapidly increasing in value in relation to the dollar.

Figure 7. Screenshots of tweets by Bitcoiners, taken on 24.12.2017.

Incorporating tokens into the protocol in some senses seemed to be working; the Bitcoin community was seemingly gaining economic independence and the blockchain/cryptocurrency ecosystem was rapidly expanding. For many who bought cryptocurrencies at the time, the volatility of the exchange rates provided an opportunity and were indeed a positive feature rather than a negative. Along with the increasing attention and fascination with blockchain technology and the news stories about the market spikes, a plethora of new cryptocurrencies started to be launched. Two problems faced by anyone wanting to launch a new decentralised cryptocurrency are firstly, you have to have enough capital and capacity to actually develop the architecture, and secondly you have to establish a decentralised network of miners and nodes to secure and run the new currency. And so,

[125] See https://www.robinhoodcoop.org/#what.

arguably one of the most widespread applications of Ethereum to date has been for so-called Initial Coin Offerings (ICOs) whereby new cryptocurrencies can 'bootstrap' the Ethereum blockchain to launch their own projects. Because the Ethereum platform requires tokens as a means to run a DAO, these were designed such that they can be deployed easily through what is called an ERC20 Smart Contract. By creating a token on the Ethereum platform, new cryptocurrency projects could sell those tokens in the expectation that they would be worth something down the line when the tech would be built, essentially raising the capital for it before almost any code has been written. Ethereum became the platform to bootstrap money creation. The easy creation of new tokens with the Ethereum ERC20 contract, and the broader attention that cryptocurrencies and blockchain technology was getting at the time due to the volatility of exchange rates. meant that a plethora of new currencies and projects were being launched and marketed, many of which were outright scams, causing a regulatory backlash against ICOs.

At the same time, it was also becoming clear that the increase in price and the speculative behaviours ran counter to the intended uses of the systems. Volatility makes it hard to use Bitcoin as money to pay for goods rather than as an investment, and makes it difficult to run applications on Ethereum. A response began to emerge where Bitcoin 'the currency' was separated out from Bitcoin 'the technology', a distinction that was mirrored in other blockchain projects looking to distance themselves from a potential impending crash in exchange rates.

> it is important not to confuse the two: Bitcoin the technology, vs. bitcoin the network, vs. bitcoin the protocol vs. bitcoin the currency. So you know as far as I am concerned, bitcoin the currency is interesting, it pulls in the media attention and at the current price it is fuelling adoption, but it is almost entirely irrelevant to the much more important topic of Bitcoin the invention of a technology that fundamentally disrupts the status quo in a couple of very important industries and also as a technology cannot be uninvented.
>
> – Antonopoulos, A. in video interview with Kantor, T. December 2013, private archive footage

In this quote from an interview with Bitcoin entrepreneur Antonopoulos the distinction between 'the technology' and 'the currency' insinuates not only a distinction between the bitcoin currency and blockchain as a technology more generally, but also an understanding of blockchain as something more long-lasting with a more sturdy and significant impact than the unpredictable and fluctuating price of the currency. Bitcoin developers and supporters that wanted to distance themselves, and the project, from the unpredictable consequences of the wild speculation and fluctuations taking place as well as accusations of Bitcoin being a Ponzi scheme sought to distinguish the underlying technology from the performance as a currency. But this distinction is not so straightforward, and there are several reasons why the speculative tendencies and volatility of Bitcoin cannot be dismissed as a fictitious, fickle by-

product of the more 'real' technological contribution. Firstly, as Bitcoin entrepreneur and author Antonopoulos also mentions in the interview that the rapid increase in value on the currency markets had the very real effect of driving adoption by attracting attention and media stories – a form of profit-driven crowd-funding that works in a trustless manner such that you don't need to believe in the technology, or support its vision in order to buy into it in the hopes of making a lot of money and thereby supporting it materially. Secondly, as mentioned above, it acted as a major fundraising exercise for development of the entire blockchain industry, and thirdly, the tokens form an important aspect of the protocol itself, giving rise to the field of cryptoeconomics, which in fact is exactly based on the inseparable relationship between economic concepts and the technology. But finally and more significantly perhaps, the architecture itself has an economic design that is likely to have impact on the volatility of the price. To fully distinguish the technology from the currency would deny and sever further research into the relationship between exchange rate fluctuations and the design and engineering of 'the technology'. The protocol design, after all, encodes a set of economic ideas, including about where value comes from, no less, and so is likely to have an effect on the ways in which plays out in currency markets. More careful economic designs are only recently being addressed more explicitly, through efforts towards so-called stable-coins (Blockchain, 2018) that are, for example, tethered to other government-backed currencies in an attempt to ensure stability. In this sense, token-based platforms are beginning to look less like decentralised initiatives that allow a certain autonomy from existing systems, and more like another layer that interacts with existing systems in complex ways that require more careful attention both in terms of analysis and design.

Incorporating a token and token economy into decentralised protocol designs opens up new fundraising and economic possibilities that are still being experimented with, but it does not in any straightforward way make the infrastructure more economically self-sustaining. Although a deeper political and economic analysis of these economic dynamics is beyond the immediate scope of this thesis, it is worth giving a brief overview of what they look like: firstly, mining rewards double as a money creation and distribution mechanism, but depend on exchange rates in relation to, for example, energy costs for their profitability; secondly, fees for verifying blocks have become another area of research and development of economic incentives; third, cryptocurrency exchanges, trading platforms and apps are where people who are not necessarily a peer or a node can purchase tokens, and are also a main site of regulation; and finally Initial Coin Offerings (ICOs) have operated as something between crowd-funding and unregulated securities issuance, and became for a few years the main economic model through which new blockchain and cryptocurrency projects would launch. Each of these face issues that are being addressed in the cryptocurrency and blockchain industry. Mining is incredibly wasteful in terms of energy, and has a tendency towards centralisation. In response, new consensus mechanisms (see for example proof-of-stake or

non-consensus-based systems) as well as hardware designs seek to rectify these two main issues. Fees entail pricing issues, whether these should be dynamic or not and an issue around willingness to pay in the context of the ingrained habits of free online services. One of the arguments for peer-to-peer payment systems was that costs would be minimised by eliminating third-party intermediation – a promise that current fee structures are disappointing. Exchanges have had some major fraud cases, and have become sites of, for example, KYC and AML regulation or alternatively are becoming decentralised themselves as a means to circumvent regulation. ICOs in turn became one of the main areas of fraud and have been banned in multiple countries. These token-enabled economic mechanisms have turned out to be hugely problematic in the long term, and the fluctuating exchange rates severely impede the aims of token economies as enabling financial sustainability of decentralised infrastructures. But when considered over time, they have nevertheless played a significant role in raising interest, funds and attention for a broader agenda of decentralisation. The question is whether there is enough clarity around what decentralisation is supposed to achieve, politically, socially and technically, for it to continue to matter when exchange rates drop and complications arise.

If decentralised, token-based infrastructures were to contribute to an economic and political disruption of existing surveillance-based internet business models, there would need to be more deliberate consideration and design for the diversity of economic interdependence with existing systems. The future shape and conditions of internet provision and governance could potentially be disrupted by decentralisation and might very well be determined by new economic ideas and business models. Token systems are a potentially powerful accounting method for distributing and remunerating the cost of running a decentralised infrastructure, but there is significant work still to be done in order for token systems to make sense in terms of establishing some level of autonomy economically and financially, of establishing what their appropriate uses are and when they simply add unnecessary complexity, scarcity and volatility, in particular in relation to the interfacing economies of fiat currencies, resources, raw materials and efforts that sustain a given infrastructure. Such agendas would benefit from shift of focus away from internal coherence of proposed systems towards their dependencies and a deliberate articulation of the kinds of relationships they are intended to enable.

My argument is that what matters for those involved in Ethereum development is not primarily any particular political or economic ideas or ideology, but instead should be understood as a particular sensibility coming out of the history and experiences of network computation. The sensibility has come out of network computer systems and the idea of decentralisation as a neutral substrate because it eliminates the possibility for control by any single set of interests. This sensibility does have political and economic effects, but these are not straight forward or easily mapped out. Such a technical proposition for tackling the dominance of major platform

businesses in the meantime is attractive for both those critical of platform capitalist business models and those who seek a new competitive angle to 'disrupt the disruptors', looking for platforms that might provide a more profitable environment for new applications and services. The broad appeal of the potential of 'decentralisation' has therefore been a powerful attractor to the agenda and proposition of Ethereum and blockchain. The particular anti-authoritarian understanding of decentralisation does, in the meantime, open up some important political possibilities. The focus on authority, censorship-resistance and privacy in earlier decentralised systems extend in important ways that disrupt established models of digital network governance and economics; a critique of authority at the basis of decentralised designs implies that protocols remain open source and open to some degree, that privacy concerns are prioritised and also that data, protocols and infrastructure are governed in ways that are transparent and at least to some extent decentralised (see 5.1.3 and 6.3). Such conditions go a fair way to ensuring that protocols do not become the same model of monopoly platform businesses, but instead either have to significantly innovate in terms of economic sustainability and/or draw on non-profit, potentially commons approaches. These developments are in no way guaranteed, however, and decentralised platforms might very well also become substrates for centralisation of wealth and power while placing huge barriers to for example accountability and oversight. Platformising decentralisation might not disrupt capitalism as such, but it does imply a sensibility that could pose a significant challenge to existing Internet business models by decentralising the control of data. The question of what kinds of business models such architectures would make possible, and what indeed would be desirable has, as of yet, not been answered.

5.2.2 Tokenised decentralisation

The incorporation of financial incentives into the Bitcoin security model turned out to be hugely generative and with Ethereum sparked a 'tokenisation' of decentralised protocols, which conversely opened these up for economic dynamics and unforeseen complications. Tokenisation, on the one hand, presented an opportunity to articulate decentralised information and communication systems that might be sustained by new kinds of business models, thereby posing both a technical and economic challenge to existing surveillance-based infrastructures of the internet (Zuboff, 2015). On the other hand, it presented two major challenges: tokenisation also introduced new kinds of complexity deep into protocol designs in ways that exceed purely technical concerns, opening these up for all the complexities of economics and finance – and on a more fundamental level, token creation brought with it the tools for engineering scarcity in the otherwise infinitely replicable digital space. The latter in the meantime also caused a change in the economic ideas and assumptions of peer-to-peer decentralised technologies in which property and defining access conditions became a main focus. Where Bitcoin had been an application-specific proposal for a payment system,

Ethereum generalised tokens into a form of 'fuel', a substrate for running any kind of decentralised application, cryptocurrency, platform or organisation. Economic concepts entered into the toolbox of decentralised systems engineers, opening up new areas of computational research. Here I discuss these two implications of tokenisation as a further extension of a blockchain sensibility, namely the complexities in field of cryptoeconomics and a shift in political economic sensibility within the development of decentralised systems before concluding the chapter.

The complexity: cryptoeconomics

> I think of cryptoeconomics as a methodology for building systems that try to guarantee certain kinds of information security properties.
>
> – Vitalik Buterin, Ethereum[126]

> The reason we are talking about incentivisation is that this ethos that seems so amazing wont work unless the cryptoeconomics incentivisation piece works, right. The idea is not good enough unless everybody says actually that is a good deal for me and we want to tune the system so that everyone will think that it is a good deal to participate and at the end of the day the overall group is better off.
>
> – Jon Choi, in December 2017 presentation on Cryptoeceonomics and Casper[127]

The incorporation of tokens and economic incentives as an integral part of the Bitcoin protocol design gave rise to what is called cryptoeconomics. Expanding on the concept of Bitcoin mining rewards and their security function – making it more profitable to contribute to the network than attack it – this budding interdisciplinary field is concerned specifically with designing incentives in such a way to ensure the secure running of decentralised systems. As Choi explains above, the main idea is to align the economic interests of an individual node/contributor with that of the system, drawing on and operationalising concepts from economics, game theory, cryptography and mathematics (such as probability). The incorporation of economic concepts into security modelling and decentralised protocol design is becoming an area of research and development in its own right across computer sciences departments and in the fields of information security and cryptography (Buterin, 2014; Garay, Kiayias and Leonardos, 2015; Kiayias, 2015; Bano *et al.*, 2017; Choi, 2017; Ethereum Foundation, 2017), beginning from the seemingly simple solution in Bitcoin, incentivising contribution in the network by rewarding bitcoin miners, incentive design and the ambition of aligning the behaviour of individuals with that of the system quickly becomes very complex.

[126] See https://youtu.be/pKqdjaH1dRo 1:46 - 1:56
[127] See https://youtu.be/6iEpqbACLbY 11:19

Figure 8. 'Miners just follow the money, and they will definitely not attack the source of their income'. Tweet by DigiEconomist 14 Oct 2017.

This tweet is typical of the ways in which game theory is drawn on in order to assess what kinds of behaviours might happen in the system given certain conditions. The argument is that although bitcoin mining has become centralised, if miners were to take advantage of this, they would face a backlash from those expecting Bitcoin to be decentralised, who would then leave the network in favour of a different cryptocurrency, resulting in fewer transactions and a lower bitcoin value. Incentives are here mobilised in order to guarantee a (commercial) concern for the legitimacy of one's actions in a game theoretical speculation on the behaviour of miners. In other words, the security model in cryptoeconomic designs attempt to take into account various kinds of incentives or disincentives for behaving in certain ways.

Cryptoeconomics is a field concerned with the design of systems whereby certain behaviours are made desirable through rewards, undesirable through punishments or impossible through code and cryptography. It is, in a sense, a complex endeavour of shaping a landscape of possible and desirable actions, indeed an attempt at a form of protocological control rather than disciplinary control (see 4.1 and Galloway, 2004). Ethereum and blockchain more generally are intended to be net neutral, meaning the infrastructure is open for anyone to use and participate in. The protocol is, in this sense, understood to be politically neutral, instead providing a substrate for any kind of protocol, currency or governance system to be built. This means that cryptoeconomics and incentive design tend to be discussed and addressed purely as security questions – how to prevent or discourage 'malicious' behaviour and encourage 'honest' behaviour. Security concerns are considered neutral concerns, pertaining primarily to the survival, benefit and coherence of the system itself. But in open, decentralised protocols, the question of what is beneficial or not, what might be considered 'malicious' or 'honest' behaviour can be contentious, and the question of who gets to decide this even more so. For example, it's up for debate whether a given action might be considered an 'attack' on the

system, or simply another understanding of how the system should work, and even more importantly, where the limits to such considerations might lie – and at what point cryptoeconomic designs begin to resemble attempts at large scale behavioural engineering. This raises the question of protocol governance; who gets to write the rules of the system and who gets to design the landscape (see Chapter 6).

A second complication in the field of cryptoeconomics is the implication of incorporating the full range of economic dynamics into the protocol design and security model. The concept in Bitcoin was to incentivise mining in the network, such that this task would be more attractive and profitable than attacking the network. But this seemingly simple idea quickly becomes quite complex in attempts at measuring or assessing. Even calculating the profitability of mining involves a number of more or less understood variables: the cost in terms of energy consumption and hardware which needs to be weighed against the potential for reward in terms of the likelihood of computing the nonce for a block, which gets further complicated by the competition with other miners and the addition of mining pools, ASICS and so on. Calculators have been cobbled together in order to be able to determine the profitability of mining.[128] That covers just the economic complexity of just one actor, namely the miner – which in turn needs to be understood in relation to the broader economic dynamics such as exchange rates, concentration of wealth amongst so-called 'whales' potentially manipulating the markets, the overall money supply and so on in order to achieve an understanding of the full security implications. In such conditions, it becomes very complex to model with any accuracy whether and when it is more profitable to contribute to the system than attack it, raising the question of what economic incentives really do in decentralised protocols and might contribute to in the long run.

Once there is economic value in the network, generalising the incentive to contribute, it conversely also generalises the incentives to attack the system and has become an intensive area of modelling, testing, research and development, in order to anticipate attacks. In Ethereum, research is focused in particular on the security issues of shifting from the Bitcoin proof-of-work consensus algorithm to what is called proof-of-stake. Proof-of-stake employs the idea of placing an economic 'stake', and the threat of losing that stake, to secure the intentions of nodes in the network instead of mining. The Ethereum project has (as of 2019) two different pathways for moving from a proof-of-work to a proof-of-stake consensus algorithm, one that is developing an interim step in which a proof-of-stake layer will be added on top of the existing proof-of-work-based network, and another that would be a direct transition to proof-of-stake. The change is far from simple, as the individual behaviours in relation to new economic conditions need to be carefully modelled, and the effects of these on

[128] See for example https://www.cryptocompare.com/mining/calculator/btc and https://www.coinwarz.com/calculators/bitcoin-mining-calculator

the overall system need to be assessed and calculated to arrive at any idea of the security properties or potential attack vectors involved. Researchers and developers working on this transition fully acknowledge that significant assumptions have to be made and that the system tends to get very complex, evident here in Ethereum developer Floersch's explanation of the new protocol called the 'Casper' version of proof-of-stake:

> We have this complex behaviour emerging from really simple economic rules, right, and this actually not specific to Casper by any means, this is any protocol that we are messing around with economics we are going to have people spending their lives trying to break it, there is crazy stuff happening, so we need better tools for evaluating these economic incentives. If we don't' actually have the right methodologies for coming up with these kind of attacks that we might face we are not going to be able to properly defend our protocol.
>
> – Karl Floersch on Casper and proof-of-stake, 2017[129]

Economic incentives, then, both increase the incentives for attack and vastly expands the potential attack surface. (This contradiction, whereby economic incentives are supposed to solve security problems but in the meantime significantly increase the attack surface is resolved somewhat in a similar manner as control, discussed in the second half of chapter 4, through the idea of complex behaviour and emergence). What Floersch means by people 'spending their lives trying to break it' is that when there is economics involved and money is at risk, the system is likely to have a lot of attacks. Indeed, as he also states, the field quickly becomes very complex. To give an example of this, in the proposed Casper (what became known as *Casper FFG*, (Buterin and Griffith, 2017), the idea is that the proof-of-stake layer will have a 'checkpoint' every 50 blocks with the underlying proof-of-work blockchain. At this checkpoint, validators put ether into a Smart Contract, verifying a given state in the network. If there are two conflicting states at the checkpoint, a third of deposits will be slashed as a punishment for the delay in finalising a state in the network. This is one of the so-called 'slashing conditions' that outline what behaviours are not permitted and therefore would result in funds being destroyed. In the case of conflicting states, the economic penalty increases the longer it takes to finalise a state, and conversely, when a state is arrived at, validators receive a reward. It is worth considering a few of the economic and behavioural calculations that would need to happen in order to understand the potential outcomes of this system: whether the loss of a third of funds is enough of a deterrent to prevent attacks; whether the punishment is too much so that it deters 'honest nodes' from wanting to be validators; whether conflicting states will occur frequently, causing so many funds to be slashed that it affects the overall money supply; whether money supply affects the value of the token on exchanges; to what extent this affects the uses of the system for applications built on top of it;

[129] See https://youtu.be/ycF0WFHY5kc 12:18

whether creating deliberately conflicting states at a checkpoint will be used as a potential attack; whether attackers are willing to burn funds to do so, draining the economy and preventing finalised states; whether 'honest' nodes would pledge a willingness to burn a similar amount in a public contract to continue securing the network regardless; whether people using the system would be satisfied with such an assurance; whether other options, like redistributing the funds to honest nodes rather than slashing (and burning) it is viable and economically possible.

This seemingly simple idea – to use the economic self-interest of actors in the network to ensure that it is more lucrative for them to contribute rather than attack the system – very quickly becomes quite complex as the tokens that are used as incentives enter into further economic dynamics. It is a field with plenty of new ideas of how to apply economic concepts to computational security, but with systemic ramifications that are not very well understood yet. Navigating economic decisions in protocol design have so far been considered primarily for network security questions and incentives as a form of behavioural engineering for security purposes. This helps to delineate some core priorities and primary concerns in design considerations that might otherwise be hard to contain. And yet the impact of these decisions cannot be simply isolated network security concerns; a cryptoeconomic design decision is simultaneously an economic, monetary and financial decision that will also affect the price of running Smart Contracts and dApps (decentralised applications), and therefore immediately impacts and shapes the potential business models that might come out of these designs. These complexities are no less than the grappling and expansion of a blockchain sensibility, operationalising other fields and dynamics in the process.

The change: from pirates to police

Finally, I would like to suggest another, rarely commented on consequence of tokenisation, namely a shift in the economic aims and ideas prevalent in blockchain notions of decentraliation. Early generations of decentralised technologies from the late '80s through to the early '00s employed decentralisation as a strategy to make a given system resilient against potential legal persecution. In peer-to-peer network culture at the time, a critique of intellectual property circulated based on the idea of digital copies as next to zero cost and infinite, and therefore naturally abundant (cf. Arvanitakis and Fredriksson 2016). File-sharing communities resisted digital rights management technologies as an artificial imposition of scarcity on information, knowledge and digital goods, epitomised in the slogan 'information wants to be free'. The infinite replicability of 'the digital' formed the intellectual justification for file-sharing and digital piracy. Networks were spaces of free flows of abundant knowledge and information, entailing multiple pathways that would circumvent any attempt at blockage or control. Because code, information and knowledge have no inherent scarcity, there had been

an underlying critique of, in particular, intellectual property rights and any attempt at forcing scarcity on abundant resources. Bitcoin marked a significant shift in this history of peer-to-peer network politics, a shift to an economic position that could be said to be the exact inverse – concerned with the expansion of what might be deemed property, building some of the most fine-grained IP management systems aimed at immediate and 'unmediated' policing of property rights (see for example Mattereum and Slock.it).[130] [131] Through Bitcoin, cryptography went from being a tool to ensure privacy to determining ownership more broadly. For the purposes of establishing a peer-to-peer payment system, this was necessary in order to prevent infinite replication of token records, thereby rendering the payment system meaningless. But in the meantime it has had major implications across several different scales and has significantly changed the very culture and assumptions of peer-to-peer in ways that have not been sufficiently acknowledged and understood. When Ethereum platformised and generalised aspects of the Bitcoin protocol, the ability to determine ownership and access control was an engrained logic and set of use-cases. Smart Contracts could become the means for fine-grained control of access to uniquely defined digital objects, determined in a ledger. The proposition of replacing aspects of payment systems, contracts, identity registration and legal enforcement with a decentralised version of these has drawn those who might previously have been critical of the very techniques of such state and economic institutions into their reinforcement in and through digital technologies (Käll, 2018; Manski and Manski, 2018).

There are nevertheless important legacies from earlier generations of peer-to-peer with an affinity to open sharing of especially knowledge: educational material and code tends to be open and shared widely, and there is a culture of leaking if relevant information is being withheld. So while Ethereum and blockchain assemblages are rarely critical of questions of private and intellectual property rights or capitalism more broadly, these sensibilities and their encoding in protocols and architectures pose some complications for what are called surveillance-based business models (Zuboff, 2015). Herein lies the potential for disruption that can in part be traced back to the political sensibilities of earlier decentralised systems. For example, most major blockchains are fully public, what has since been called 'unpermissioned blockchains', meaning one does not need special credentials or permissions to take part in the network and browse the data. This poses a problem for many types of business that would rather keep most of their operations and agreements relatively private.

Such approaches to decentralisation and openness are justified through network security issues and privacy concerns rather than a consideration of the socio-political effects of different property regimes. In the meantime, so-called permissioned layers have been added

[130] See https://mattereum.com/
[131] See https://slock.it/

so that new types of privacy arrangements can be established (cf. Didil, 2017). These layers add the potential for fine-grained management of privacy and transparency that would be better suited to existing business needs. In order to facilitate research and development for how Ethereum might be useful for businesses and industry, the Enterprise Ethereum Alliance was formed, with nearly 500 companies and institutions as members, ranging from tech companies like Microsoft, to Antibiotic research UK, Credit Suisse to the Government of Andhra Pradesh in South India, Singapore University of Social Sciences, Santander, BP, Shell, American Family Insurance and many more, including blockchain start-ups and Consensys.[132] The Alliance is also a non-profit, but is set up to support research and development of Ethereum-based applications specifically for industry, including exploring permissioned uses of the otherwise unpermissioned Ethereum chain. While the Foundation applauded the formation of the alliance, it retained independence from it.[133] [134]

Neither privacy and transparency, nor new, open business models are therefore guaranteed by the protocols. New layers are developed on top of such systems that can exacerbate or ameliorate issues of data and privacy as well as issues around Intellectual Property, ownership and access. There is an implicit arrangement of commons, public and private economies, but also some significant areas of negotiation over appropriate economic and property regimes currently taking place. And so much of the political-economic potential and outcome of decentralised systems is very much up for negotiation. But it is a negotiation and developing sensibility that prioritises security in decentralised network computation, as these are considered to be a neutral starting point.

The ability of cryptographic tools to determine access conditions maps well to existing understandings of property and allows for very fine-grained determination of property relations, and so has a momentum of its own. The political sensibilities and affiliation of the current generation of decentralisation movement are grounded in decentralised networks rather than particular economic and politically informed ideas. And so, just as with capitalism more generally, there is not an explicit critique of state technologies either beyond notions of centralised control. Instead, the determination and enforcement of property and identity are let lose as tools for anyone to use, determine and define in ever more fine-grained manners; many technologies, concepts and frameworks from what might otherwise be understood as centralised entities to be deployed in new decentralised ways as the political, economic and legal is addressed from the perspective of the decentralised computational network rather than the other way around. Notions like security, property, sovereignty and so on are not scrutinised per se, but instead are sought to be decentralised such that these are no longer

[132] See https://entethalliance.org/
[133] See https://entethalliance.org/ footer stating independence between the Alliance and the Foundation.
[134] See https://cointelegraph.com/news/ethereum-alliance-formed-by-microsoft-intel-ubs-secures-support-of-eth-foundation

determined and enforced by a state, but by potentially anyone. The effects of decentralising existing economic and financial technologies cannot be easily predicted, because they do open up tools of digital security and enforcement that was previously out of reach. But this has entailed a shift from a culture of pirates circumventing authorities, to policing and enforcement of property and through designing automated algorithmic authorities.

5.3 Conclusion

What holds a blockchain assemblage together, the common sensibility across the field, is not concerned or unified by neither the disruption of, nor propagation, of right wing capitalist ideas. Yet there are aspects to the ways in which such a sensibility does present a redistribution of the sensible, through which new things come to matter that have the potential to disrupt existing digital economies and business models, challenging existing sensibilities. In this chapter I have traced through and described a blockchain sensibility. Drawing on Rancière's notion of disruption and redistribution of the sensible and Barad's articulation of an onto-epistemological *making into matter what matters*, the sensibility I have traced comprises the assumptions and ideas of what matters in the assemblage. I employed Gibson-Graham's notion of diverse economies (2008), initially when approaching the blockchain assemblage and analysing it through the history of decentralised architectures. This enabled me to shift the focus from concerns and questions of capitalism to a broader as well as more specific interrogation such that other matters might come to light. I drew on the idea of diverse economies once again when approaching questions of tokenisation from within a blockchain assemblage, such that relations to already existing economic spaces in, for example, exchange rates are addressed rather than sidelined as not mattering. I acknowledge that this might be considered somewhat of a misappropriation of Gibson-Graham's intentions and agenda, as, arguably, my analysis stays within the bounds of established and formal economics rather than discussing the diversity of for example social currency projects in blockchain nor, for example, their feminist approach of highlighting dependencies on externalities, materials extraction or unpaid labour. This has largely been because the aim of this chapter has primarily been to articulate a sensibility of the blockchain assemblage and to do this in order to point towards the edges of what matters in such a sensibility. The aim, in other words, has *not* been to argue for more inclusion of things otherwise not perceived as mattering (whether exchange rates, unpaid labour, materials extraction and so on), but instead to make visible the particular nature of this kind of sensibility, that, in turn, would allow for other sensibilities to sit alongside and shift the focus of attention and analysis to their relations. In short, the aim is not inclusion (inclusion and externalities are a condition of

assumptions of a singular sensibility) instead to articulate as *specific* what otherwise tends to be described as general – in the case of blockchain, computation and markets.

To conclude, what holds the assemblage together is not primarily particular economic, nor political affiliations, but an affiliation with decentralisation as articulated in and through network computation. It is an understanding and operationalisation of decentralisation that stems from earlier peer-to-peer histories of developing decentralised architectures in order to circumvent authorities. The history of peer-to-peer and cryptography in the Cypherpunk movement in particular in the US and UK had entailed severe legal and personal consequences for those involved (Coleman, 2009, 2014), in which inordinately harsh sentences had been passed on digital and information activists.[135] These experiences solidified the understanding of central government as violent and coercive and the law as acting in favor of big business interests while also enforcing the idea of the need for peer-to-peer networks to resist these. The purposes in early decentralised design were particular, practical and usually well understood by the communities building, sustaining and using a given system, namely to make systems that would be resilient to targeting by authorities. I have argued that the context of the financial crisis and the specific Wikileaks case gave Bitcoin and decentralisation a more general appeal as a disruption to existing economic and political institutions and processes. Along with Bitcoin, an emphasis from Cypherpunk culture also emerged and became a more broad tendency, namely the importance given to *technology-based* solutions to problems of power, not only as a tool for resisting particular governments and agendas but as a general proposition in and of itself. Technological networks would be independent of not just government control but also the control of potentially corrupt human beings more generally, and would provide a (net) neutral substrate for decentralised communities to form.

I have drawn on this pre-Bitcoin history of decentralisation in order to explain the very specific ideas and justifications for blockchain. I have argued that in the years since the invention of Bitcoin and in particular through Ethereum, two major shifts happened in the development of such decentralised architectures, namely their generalisation into platforms and their tokenisation, both of which have had major effects as decentralisation changed from a strategy to a general sensibility. I argue that an overlooked detail in these experiences is very important for understanding what was to become a generalised blockchain sensibility, namely an affiliation with the system over and above what happens to those using it. Decentralisation had been effective for ensuring the survival of the system in the face of authorities, but not necessarily the individuals running nodes or using the network who might very well be arrested, scammed or targeted in other ways. This, I argue, is a legacy from early

[135] See for example the story of Aaron Schwartz (Schwartz, 2013)
https://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html

decentralised systems design that was generalised with the Ethereum project of making the Bitcoin architecture Turing-complete. It is an approach to systems design that has had a major effect on the use-cases and sensibility of blockchain projects ever since, and can be seen in the particular understandings of trust, authority, control and autonomy. The system design itself is considered trustless, while for those using it, it indeed requires a lot of trust; the system should be decentralised so that it is beyond control by any authority, but authority, in a generalised system, is anyone who might control the system, therefore the system itself needs to be built such that it is beyond the control of anyone. Autonomy, therefore, is autonomy of the network system, ensuring it is beyond control – a generalised autonomy, rather than self-determination and more control for a particular community. The generalisation of an operationalisation of decentralisation from earlier peer-to-peer strategy, where conditions and truths are determined primarily for the system, has caused confusion, conflating systems designs with social and political effects, but also been very effective in attracting support, interest and efforts across political spectrums.

Ethereum also generalised tokens as a means for coordinating and operating decentralised computation. In what I have discussed as 'tokenisation' I traced how Ethereum turned the specific application of Bitcoin as a payment infrastructure into a platform fuelling any potential computation rather than just transactions. Instead of discussing the merits of this approach from a critique of capitalism, I draw out and discuss the particular form of disruption that this was intended to initiate, namely as a system that would pay for itself and therefore undermine the existing business models currently sustaining the internet. I draw again on Gibson-Graham, however, to point towards the ways in which otherwise sidelined issues of other economic spaces continue to matter and complicate such hopes for economic autonomy, with the explicit example of dependence on exchange rates. I argue that this is not only a dependency but, also, by being incorporated into the protocol, complicates the design and modelling in the emerging field of cryptoeconomics. Finally, I discuss a broader shift that the generalisation of tokens has brought about, namely a shift in the culture of peer-to-peer from an understanding of digital networks as fluid spaces of abundance towards ever more fine-grained determination and enforcement of property. In a sense, the tendency has been towards decentralising techniques of both state and markets in ways that are more complicated than simply replicating these. In the next chapter, I describe two major events in Bitcoin and Ethereum that challenged and caused a reassessment of how a blockchain sensibility might best be materialised, putting into question the appropriate role and limitations of algorithmic means for organising consensus.

6 Dissensible matters

In this chapter I propose the concept of the *dissensible* to describe a persistence of incompatible sensibilities and to look at the ways in which dissensus and incompatibility are negotiated in Bitcoin and Ethereum. The Bitcoin consensus algorithm had inspired a whole new field of engineering decentralised protocols based on the idea of algorithmic means for organising consensus in decentralised networks. Bitcoin and Ethereum were intended to be 'trustless' – neutral protocol substrates, algorithmic rules, on top of which all manner of differences or any form of political or economic systems might be designed and play out. Such consensus algorithms determine a form of consensus for the network, but as it turned out, the sites of disagreement, differences and dissensus, the question of the political, shifted to protocols themselves, their design and maintenance. In the previous two chapters, I have described the concepts and ideas that are operationalised in blockchain, and the histories and experiences that gave rise to these specific understandings of concepts of decentralisation, trust, autonomy and neutrality. The political in relation to the technical might be understood as the construction, materialisation and automation of particular social, cultural and political concerns (Daston and Galison, 1992; Latour, 1992; Feenberg, 1999; Star, 1999; Paul N. Edwards, 2003). But the proposition of blockchain distinguishes itself from other technologies in that it seeks to intervene into the very processes of political determination; not only as an expression and materialisation of, but also as a proposition for, different agencies through which to negotiate the political, suggesting the involvement of algorithmic determination in governance, the very process of negotiating and settling differences. If blockchain protocols suggest a new resolution to the political, determining how decisions are made, then in the words of Kreutler, 'Who is responsible for making the decision on how to make decisions?' (2018). This question became pertinent in and for blockchain assemblages over the course of major conflicts about protocol changes in both Bitcoin and Ethereum. In Bitcoin, a long-standing question around scalability, known as the *Bitcoin scaling conflict*, culminated in the network 'forking' in August 2017, splitting into two different cryptocurrencies. In addition, after what became known as The DAO hack, the Ethereum Foundation decided to fork the blockchain in 2016 in what some saw as a betrayal of the claim of immutability and autonomous code raising questions around governance of the Ethereum protocol.

Challenges to the assumed consensus in the network turned what were otherwise perceived as purely technical issues into politicised debates and raised questions of what holds blockchain assemblages together and how they come apart when differences and incompatibility turns out to be unresolvable. By tracing dissensus and incompatibility the limits to algorithmically-determined consensus in open decentralised networks present themselves: open, decentralised networks can be designed in many different ways and these differences are not only a matter of what 'works' best technically but also for who or what it works, who

benefits most from a given change to the architecture and who gets to determine and enforce such changes. In Bitcoin and Ethereum, the concept of 'decentralisation' was mobilised and operationalised alongside cryptography in order to determine and enforce consensus without resorting to authorities, and yet, decentralisation is in itself articulated and materialised in and through different mediums (networks, assemblies, chats or otherwise) and can be encoded in different ways. I discuss decentralisation as the 'fix' to this very question of 'who is responsible' in relation to literature on the political, most notably Rancière's discussions of the political as the moment of dissensus *'as the presence of two worlds in one'* (Rancière, 2010, p. 37) and Mouffe's ontological starting point of 'failed unicity' (Mouffe, 2012, p. 29), both acknowledging the ongoing possibility of incompatibility, difference and disagreement. Drawing on these notions, I critique the idea of decentralisation as a 'fix' to the political in any final manner, describing the political instead as ongoing potential for things to be different. The *dissensible*, drawing on Barad, is the onto-epistemological potential for incompatible differences to emerge and come to matter.

The chapter is structured as follows: I first describe the way the Bitcoin protocol is governed in and through a version control platform commonly used for hosting and collaborating on code projects, namely GitHub. I then describe the Bitcoin scaling conflict and the ways in which the roles and actions of GitHub as well as the emergence of more specialised roles in the Bitcoin network became foregrounded as governance mechanisms and rearticulated as such. The conflict politicised what were otherwise considered neutral technical questions about capacity and scale, these suggesting different development pathways and visions for the project drawing on different ideas of decentralisation. The Bitcoin scaling conflict resulted in a 'fork', which was to become one of the main mechanisms through which to resolve incompatible differences. In the second half of the chapter then, I first describe 'forking' as a dissensus mechanism, and then discuss the differences and implications of project forks, code forks, chain forks, hard or soft forks. I then discuss a major conflict in the Ethereum assemblage, namely The DAO hack, which was to fundamentally challenge the idea of autonomous, neutral code beyond the control of humans that had informed much of the proposition of the platform. The hack forced a reassessment of understandings of non-human determinacy and opened up for a rearticulation of these in which 'the social' would have a place. In the years since these two major conflicts, governance has become one of the major areas of focus in blockchain projects more broadly. In response, some tendencies in the field address the problem of governance as something to be solved once again through forms of code and algorithmic determinacy in what has come to be known as 'on-chain governance', while in other projects the problem is addressed through attempts drawing up the right combination of human and algorithmic determinacy with the at coding entirely new forms of societies. I would like to suggest that instead of these variations on complete solutions to governance and the political, which both assume a blank slate or complete replacement, a far more interesting

approach would be had by focusing on what a particular network-form of governance might do in relation to other already existing geo-political governance institutions – in other words, tracing the project once again back to its roots as a means for circumventing authority, less as a complete solution and replacement, and more as a new kind of space that might sit along side existing institutions and processes for political determination. This also raises the question of what more precisely it is that blockchain and decentralised governance methods can do that is different from existing institutional forms and methods of addressing the dissensible.

6.1 Bitcoin and the matter of dissensible decentralisation

> Bitcoin Core is an open source project, which maintains and releases Bitcoin client software called "Bitcoin Core".
>
> It is a direct descendant of the original Bitcoin software client released by Satoshi Nakamoto after he published the famous Bitcoin whitepaper.
>
> Bitcoin Core consists of both "full-node" software for fully validating the blockchain as well as a bitcoin wallet. The project also currently maintains related software such as the cryptography library libsecp256k1 and others located at GitHub.
>
> Anyone can contribute to Bitcoin Core.
>
> – Bitcoin Core website[136]

The quote above, from the Bitcoin Core project webpage, is a very careful description that no longer takes for granted that the people, client and repository of Bitcoin Core is *necessarily* 'Bitcoin', although for all intents and purposes it is, in the sense that the project maintains the **reference client** that most of the network is running.[137] This understanding, that *Bitcoin Core* is not in any easy or straightforward way 'Bitcoin', but instead is a specific project in and amongst other *potential* versions of Bitcoin, has been one of the consequences of the scaling conflict, a major unresolved dispute over a technical decision that would have longer term ramifications for the development pathway of the project.[138] The Bitcoin scaling conflict made evident that the consensus protocol does not in itself resolve problems of dissensus and does

[136] See https://bitcoincore.org/en/about/ [accessed 27.11.2017]
[137] See also https://bitcoin.org/en/about-us#owntxt4-title describing how 'Bitcoin.org is not Bitcoin's official website. Just like nobody owns the email technology, nobody owns the Bitcoin network. As such, nobody can speak with authority in the name of Bitcoin.'
[138] As of 2018, still very much an open dispute.

not solve problems of power and the political in any final manner. A *dissensibility* forced debates about who or what determines the outcome of such incompatible positions. The maintenance of the Bitcoin protocol came to matter and it became necessary to articulate the governance of the protocol itself. These new articulations in turn would have to contend and comply with the main sensibilities of decentralisation, openness and consensus which in turn led to new understandings of open source protocol development processes as important governance methods.

This section first describes the distinct types of actors and modes of governance that emerged in and through the conflict as mattering politically. It is important to know a little bit how protocols are managed, updated, deployed and executed in open, decentralised systems in order to understand the ways in which these roles became politicised in the process of the scaling conflict. I then outline the story of the conflict itself, highlighting the ways in which it challenged and forced a rearticulation of claims of decentralisation and trustlessness in relation to the specific interests and concerns of the actors involved. Finally, I discuss the case in terms of how the political is once again sought to be resolved through a measure of decentralisation to not only the protocol but also governance layers. The section concludes with three main points raised by analysing Bitcoin protocol governance through the persistence of the dissensible: that 'decentralisation' can be operationalised and encoded in many different ways; that mediums of governance therefore are always necessarily particular and therefore matter politically; that any governance 'solution' is therefore necessarily particular rather than a final solution to the political. These points mean that a given architecture scrutinised not only for the extent to which they live up to a given measure of decentralisation, but more precisely the extent to which they live up to an assumed effect of decentralisation.

6.1.1 Governing open protocols

The Bitcoin protocol and algorithms are run across thousands of computers that reference and are updated from a specific repository on GitHub also called the **reference client**.[139] This reference client comprises the consensus rules of Bitcoin, meaning the rules that nodes in the network agree make up 'Bitcoin.' Until the scaling conflict, the processes and actors involved in maintaining, deploying and running the reference client were not considered to matter significantly in terms of the political aims of the project. 'Bitcoin' as a decentralised peer-to-peer project tended to be thought of through node/vector diagrams, nodes communicating directly and of relatively equal size – but as it turned out, not all nodes are the same. Specialised actors emerged with different kinds of interests, informed by conditions external to the protocol itself, for example exchange rates, the cost of electricity in a given

[139] See https://github.com/bitcoin/bitcoin/

country and so on. When the conflict intensified, these were held up for scrutiny in terms of the main principle of decentralisation, and in the security terms of trustlessness. Here, I briefly describe the different types of roles and activities involved in making changes to, deploying and running Bitcoin clients.

GitHub is the platform through which the Bitcoin reference client is managed. It is a distributed versioning and collaboration platform based on git version control systems used for many open source development projects. The platform determines a set of relationships and credentials to the repositories and content, much of which has filtered into and become a major part of how blockchain protocol governance is discussed and takes place. Code is held in **repositories**, of which a person, or limited group of people, are 'owners' and can decide on the permissions of other contributors. In Bitcoin Core there are three people, called **project maintainers** (as of early 2018 Wladimir J. van der Laan, Marco Falke and Jonas Schnelli), who have what is called **commit access,** meaning they can determine what contributions by any of the hundreds of contributors are committed (integrated) into Bitcoin reference client code (or that of other related projects in the Bitcoin repository).[140] There are several different ways this takes place – pull requests, merges etc.– which I explain below.[141]

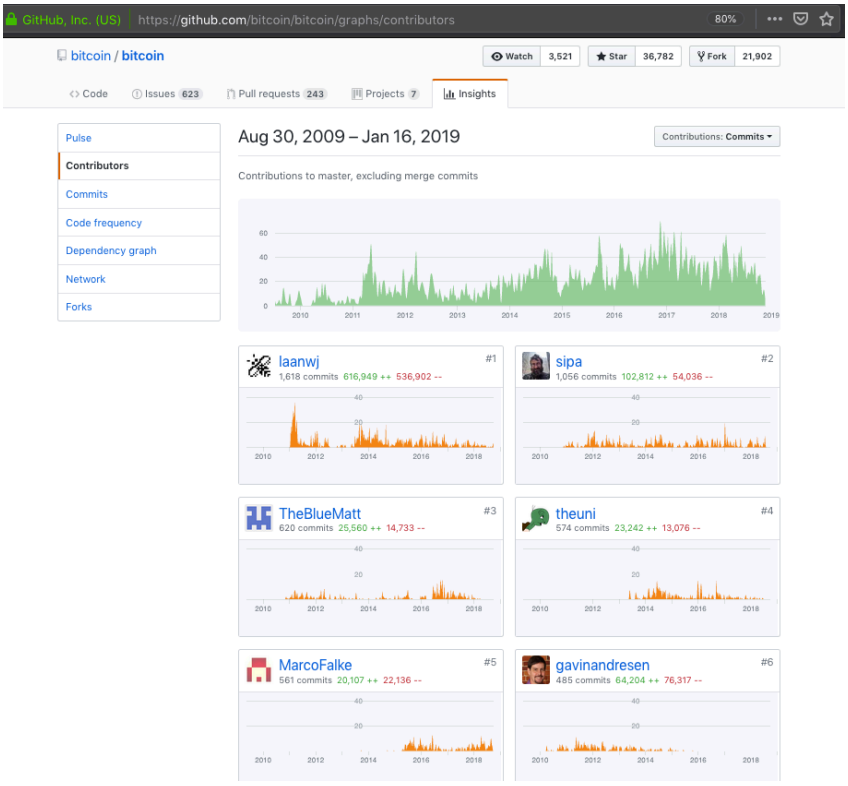

Figure 9. Screenshot of the first six in a long list of contributors to the Bitcoin reference client on GitHub from the creation of the repository in 2009 until January 16th 2019.

[140] See https://github.com/bitcoin/bitcoin/projects
[141] See https://help.github.com/articles/github-glossary/

The primary purpose of GitHub is to facilitate the management of contributions to code in such a way that these can happen openly and freely by anyone while still keeping the integrity of a given codebase (the screenshot above is of a page in the Bitcoin GitHub repository, listing contributors and their contribution statistics). Anyone wishing to contribute to Bitcoin can **fork** some part of the Bitcoin repository, meaning duplicating some of the code into a different repository to work on their own changes, experiments, patches or additions. They can then submit what is called a **pull request** with the given contribution. After a peer-review process, developers can choose to merge and commit or reject it. If rejected, the person submitting the pull request can choose to develop their own fork of the code in a new repository, meaning that they control and essentially have a version of the (Bitcoin) code that includes their amendment (see **code forking**, more on forks in section 3.2). This also means that, at least in theory although practically unlikely, Bitcoin could change hands in terms of reference client maintainers if there was consensus in the network that developments taking place in a new repository better reflect the aims of the project (for that to happen would require coordination of a large number of actors across remote geographical locations, as will become evident). The GitHub platform also keeps track of who has done which commits and when, giving an overview of contributions and transparency of who has been responsible for what aspect of the code.[142]

The process for contributing to the Bitcoin repository was further formalised by developer Amir Taaki in 2011, specifying the Bitcoin Improvement Protocol (BIP) through a first BIP0001 as a way to create some oversight and accountability in code governance, motivated by a concern regarding informal hierarchies that were emerging. The purpose of BIPs and the general code governance model in Bitcoin is meant to be managing maintenance and patches in the most efficient manner. Many of these discussions take place on the developers' mailing list with regards to why a given proposal might be suitable or not. However, those whose contributions and suggestions are rejected are not always in agreement, and there is disgruntlement about the development process being determined by informal dynamics between trusted insiders. Jo Freeman's seminal feminist text *The Tyranny of Structurelessness* was referenced in forums and debates in particular during the Bitcoin scaling conflict (described in more detail below) to raise awareness of informal hierarchies in what might otherwise be considered decentralised, horizontal conditions.[143] The BIP process was partially modelled on the Python Improvement Process.[144] To submit a BIP, one is first encouraged to discuss the idea in more informal channels and forums of the community, to

[142] See https://github.com/bitcoin/bitcoin/graphs/contributors
[143] See for example https://www.reddit.com/r/Buttcoin/comments/2bmbmi/the_tyranny_of_structurelessness_and_why/
[144] See BIP101, the proposal for how to suggest changes to the protocol https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki. This process is not unique to Bitcoin but an evolution of processes developed in open source more generally, and in this case specifically inspired by the process used in Python, PEP-0001

understand whether the idea has been suggested before or is indeed relevant before developing it further; then to email the proposal to the Bitcoin developers' mailing list, an open email list, as well as the **BIP editor** (Dashjr as of 2018).[145] [146] The suggestion might already at have been rejected before reaching status as a BIP. The BIP editor ensures that the BIP follows the formatting requirements and has the required information before it is assigned a number. The author (or 'champion' of the BIP) then submits it as a **pull request** to the BIP section of the repository at https://github.com/bitcoin/bips. It is then reviewed further by peers and merged by the BIP editor when ready.

It might seem as if developers with commit access have substantial powers to determine the direction of a protocol. However, because the code is open and reviewed by a community of developers, and a given client needs to be accepted by nodes and run across thousands of computers rather than a central server, contributors and nodes in the network have to be convinced to change over to the new protocol as and when major changes are made (cf. Wirdum 2016c). This happens in several ways, but the most powerful to date has been by convincing **miners** to adopt changes. Miners validate transactions and add blocks to the blockchain, so they can essentially decide to stop validating transactions that are made using a previous version of the protocol, and push for adoption of the new version (or the other way around, refusing the modified protocol). This decision can be relatively harmless, in the case of so-called soft forks (discussed further in section 6.2.1 below), as these types of changes and patches do not break compatibility between versions. But the case of a hard fork, in which the new version is incompatible with previous versions, the Bitcoin blockchain splits and miners play a significant part in determining which of the forks 'win' by mining on the branch that they agree with.[147] Although miners are in this way able to determine the outcome of protocol changes (a particularly problematic possibility given the centralisation of mining, discussed in 4.1.3), they are however not the only type of nodes that ensure that transactions comply with the consensus.

Full nodes are peers in the Bitcoin network that store the full Bitcoin blockchain and run a full Bitcoin client.[148] They participate by witnessing and relaying messages, checking that the **consensus rules**, i.e. Bitcoin reference client is complied with. If a transaction is not in the correct format, or attempts something that is not permitted by the reference client, it is rejected by the full nodes and will not be added to the memory pool of transactions to be mined and verified. In this sense, full nodes can also organise and mobilise in support or

[145] https://bitcoin.org/en/development website (accessed 27.02.2018) recommends irc.freenode.net #bitcoin-core-dev. Web interface: https://webchat.freenode.net/?channels=bitcoin-core-dev Logs: http://bitcoinstats.com/irc/bitcoin-core-dev/logs/2018/02
[146] See full archive: https://lists.linuxfoundation.org/mailman/listinfo/bitcoin-dev
[147] Miners can also 'signal' their support for a given protocol change, as in the case of BIP141, by hashing a little message into their blocks (in this case bit1, and in the case of BIP). See Wirdum, 2017 https://bitcoinmagazine.com/articles/bip-91-has-activated-heres-what-means-and-what-it-does-not/
[148] Also called full nodes, as they store the entire blockchain and check that the protocol is complied with.

refusal of a given change to the protocol. Full nodes emerged as a potential actor and decision-maker role in terms of protocol governance when the scaling conflict seemed to have reached a deadlock. Through a campaign for a 'user activated soft fork' (BIP 148) in 2016 organised largely through the #UASF hashtag on Twitter, people were encouraged to set up full nodes adopting a protocol change that would resolve the conflict through a compromise that would prevent the network from splitting (see *segregated witness* below). Full nodes can, in this way, participate in determining and implementing protocol changes, but are different from miners in the sense that they are not rewarded for their contribution in the network. This difference to some extent also shapes the characteristics and interests of the two types of nodes: mining is increasingly done by mining pools, companies that have begun to resemble commercial service providers, whereas full nodes tend to be run by people looking to contribute on the basis of concerns for the ethos, overall development and governance of the project.

At the height of the Bitcoin scaling conflict in 2016, the BIP process was updated and expanded by Bitcoin developer Luke Dashjr, likely in response to accusations and disgruntlement of centralised tendencies in protocol governance, in order to 'make the selection criteria more objective.'[149] Notably, the updated BIP process also included a new articulation of Bitcoin protocol governance that would justify these processes in relation to the principle of decentralisation understood in its market form:

> For Bitcoin to function as a currency, it must be accepted as payment. Bitcoins have no value if you cannot acquire anything in exchange for them. If everyone accepting such payments requires a particular set of consensus rules, "bitcoins" are de facto defined by that set of rules - this is already the case today. If those consensus rules are expected to broaden (as with a hard-fork), those merchants need to accept payments made under the new set of rules, or they will reject "bitcoins" as invalid. Holders are relevant to the degree in that they choose the merchants they wish to spend their bitcoins with, and could also as a whole decide to sell under one set of consensus rules or the other, thus flooding the market with bitcoins and crashing the price.
>
> – BIP 0002, Dashjr[150]

The argument was that coin 'holders' could wield power and determine protocol decisions through, for example, crashing the price, as mentioned above. Including such economic dynamics in the new BIP process description can be understood as a rearticulation of the Bitcoin governance, defending its decentralised nature: the argument was that neither developers with commit access, miners, nor full nodes fully determine the direction of the

[149] See https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki
[150] See https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki [accessed 08.10.2018]

project, because the project would have no value and these roles would be meaningless if there were no people doing transactions or merchants accepting Bitcoin. This argument was used in order to justify and meet the criteria of decentralisation by involving an idea of 'the economy' as part of a governance process – and so coin holders and merchants entered into a description of the balances of power and decentralised governance of the system. This remains to a large degree a claim, as the understanding of coin holders and merchants as distinct, organised and coordinated governance actors that are able to answer back to developers and miners has so far not been significant. This form of capacity – to signal disagreement on the direction of the protocol by changing to a different currency – is also likely limited by network effects. If a network is large enough, it can be near impossible for an individual to leave given that most activities are taking place through that network.

Cryptocurrency exchanges had, in the meantime, emerged as powerful entities, serving as gateways for new users to access and purchase cryptocurrencies. Decisions about whether to list a currency or not could make a big difference for the success and survival of that currency. These have the potential to play a significant role in putting pressure for a given technical change to take place. Exchanges were therefore also an obvious site of legislation (specifically KYC, Know Your Customer, and AML, Anti Money Laundering), which in turn also affected decisions about which currencies to list. But most significantly in terms of protocol governance, exchanges' handling of forks, whereby a given currency would split into several versions, also came into question. In open decentralised systems, setting the criteria for what currency is considered worth supporting or not was politicised. The emergence of decentralised exchanges took place in and around these years, in response to such questions of governance, whereby an exchange would have the power to determine the validity of a currency, as well as in response to legislation and the concomitant compromise on the principle of anonymity and perceived potential of censorship and control by authorities.

With this brief run-through of the diversity of actors and how code maintenance, updates and changes happen in Bitcoin I intend to explain the ways that notions of decentralisation, openness and trustlessness that hold together the Bitcoin assemblage form a sensibility, and are attempted to be realised not only in the protocol but also in its governance. In the following section, I describe a major conflict in Bitcoin that was to test many of these code governance processes and raise the issue of how to deal with incompatible differences. The Bitcoin consensus algorithm had, for some, solved the age-old problem of consensus without authority, the final sentence of the Bitcoin whitepaper reading: 'Any needed rules and incentives can be enforced with this consensus mechanism' (Nakamoto 2008, p. 8). But as it turned out, the consensus mechanism itself was not beyond dispute, despite being made up of cryptographic proofs in a 'trustless' architecture. I discuss the re-emergence of the political, the *dissensible*, in the sense of negotiating incompatibility in Bitcoin, and the ways in which

these are resolved while still in reference to the primary principle of 'decentralisation'. The Bitcoin scaling conflict raised the issue of dissensus, politicising what were otherwise perceived as technical questions, where the political disputes of 'mushy humans' (see Chapter 4) was supposed to have been resolved through a neutral consensus algorithm.

6.1.2 The Bitcoin scaling conflict

The Bitcoin scaling conflict can be summarised as being about how to technically accommodate for a growing number of transactions. The reference client stipulates a data limit of 1MB per block that had been put in place early in the history of Bitcoin to safeguard against micro payments being used as DDoS attack – spamming the network with many small transactions.[151] As the network and number of transactions grew, most notably two Bitcoin developers, Mike Hearn and Gavin Andresen, began to publicly express concern that blocks on the blockchain were 'filling up' in the sense that the increasing numbers of transactions meant blocks were nearing the 1MB blocksize hard limit (Andresen, 2015; Hearn, 2015, 2016; IamSatoshi, 2015; Vavilov, 2016). The worry was that this would cause delays in transaction verification and inhibit any scaling of the network in terms of capacity and numbers of transactions. In June 2015 Andresen put forward a so-called Bitcoin Improvement Proposal, BIP101, proposing to increase the data limit of the blocks on the blockchain at a steady rate, starting with an increase to 8MB, which became known as Bitcoin Classic. These ideas were further developed with Hearn into the Bitcoin XT client to replace the existing Bitcoin client, sparking divisions and outrage across large parts of the community. The outrage was largely because XT would force a hard fork of the Bitcoin protocol, meaning the changes it proposed would be incompatible with the existing reference client, and would potentially split the network.[152] XT and Classic were understood as not only a change to blocksize but also a commitment to a very specific development pathway for Bitcoin that a large number of Bitcoin developers and users disagreed with.

The position against increasing blocksize was largely that the governance and running of the protocol layer should remain decentralised, and that in order to scale the network, faster and possibly more centralised solutions and applications could be built on top (BitFury Group, 2015; Vavilov, 2016; Wirdum, 2016b). The argument was that larger blocksizes would make the load of participating as a full node in the network heavier, and potentially centralise who is able to run Bitcoin in terms of witnessing transactions and ensuring that the consensus rules were complied with; that larger blocks would result in fewer people able to run nodes. There

[151] DDOS attacks mean denial of service attacks and are usually done by overloading a system – in this case overloading the network with transactions by flooding it with micropayments. See https://bitcointalk.org/index.php?topic=1347.msg15366#msg15366

[152] See Bitcoin Core statement on hardforks and softforks and compatibility in relation to the scaling conflict: https://bitcoincore.org/en/2016/01/07/statement/ See also http://nodecounter.com/#all_nodes for a graph of how many nodes are running which protocol.

were already concerns that the centralisation of mining was concentrating power in a few hands (see image below) and full nodes had emerged as a potential counter balance to this. The dispute came to be debated as a question of trade-off between throughput (where larger blocksizes would facilitate more transactions) and decentralisation at the protocol layer (which might be compromised by a larger blocksize solution to the problem of throughput) (cf. Wirdum 2016b).

Figure 10. Screenshot of tweet by Jameson Lopp at the Scaling bitcoin conference in December 2015, demonstrating the centralisation of bitcoin mining.[153]

In order to develop proposals further and attempt to find common solutions, a major conference, the *Scaling Bitcoin workshop*, was held in Hong Kong in December 2015 gathering engineers, developers, academics and stakeholders and during which several alternative solutions to larger blocksizes were presented.[154] What came to be known as the Bitcoin Core fraction and a company called Blockstream took the position that the Bitcoin blockchain was more suited as a decentralised settlement layer. New technical proposals would accommodate other layers of development that would facilitate faster transactions, including *sidechains* (Back *et al.*, 2014), a *lightning network* (Poon and Dryja, 2015) and *segregated witness* (Wuille, 2015). The dispute was developing from a technical issue into a question of the future shape and purpose of the project, referencing different understandings of 'decentralisation', namely whether to compete directly with existing global payment

[153] See https://twitter.com/lopp/status/673398201307664384
[154] See https://hongkong2015.scalingbitcoin.org/

infrastructures as 'cash', or evolve as a new form of infrastructure altogether, potentially as a form of global settlement layer or asset class, prioritising decentralisation on a protocol layer (Wirdum, 2016b).

In the midst of the scaling conflict in the summer of 2016, an Australian businessman, Craig Wright, came forward to the media and general public claiming to be Satoshi Nakamoto, the inventor of Bitcoin, and staged a series of 'proof sessions' broadcast by the BBC, The Economist and GQ. Wright had already held 'private proof sessions' with Bitcoin Classic developer Gavin Andresen and one of the founding directors of the Bitcoin Foundation, Jon Matonis, who subsequently both published blogposts in support of Wright.[155] Both of these individuals also supported increasing the Bitcoin blocksize. The Bitcoin community scrutinised and immediately rejected the proofs as fake and demanded he sign a block or a message with a cryptographic key used in some of the earliest blocks on the Bitcoin blockchain.[156] For a community that had formed around the idea of a trustless system, Wright would have to provide evidence in the only way acceptable as secure to this community – through a valid cryptographic signature. But Wright refused 'to jump through further hoops.' This comment on ycombinator expresses the general feeling:

> Why would Satoshi go about proving his existence and identity in such a convoluted matter? Simply signing the genesis with a message and posting it pretty much anywhere (bitcointalk, /r/bitcoin, here) for people to verify is all it takes. Not a rambling blot posts full of screenshots and some back-alley interview. This is exactly the kind of 'slight of hand' that a conman utilises, not a cryptographer of Satoshi's caliber.
>
> – Forum thread on ycombinator[157]

As soon as it became clear that the proofs were fake, it was announced that developer Gavin Andresen had had his commit access revoked, stating concerns that the security of his account and/or his opinions had been hacked and that he was too close to Matonis and the Bitcoin Foundation who were perceived as cooperating closely with US regulatory authorities.[158] Gavin Andresen was the developer who had initially suggested an increase in

[155] See Matonis (2016): http://themonetaryfuture.blogspot.co.uk/2016/05/how-i-met-satoshi.html and Andresen (2016: http://gavinandresen.ninja/satoshi; here Andresen states that Wright signed a message with the private key from block 1 of the Bitcoin blockchain, see https://np.reddit.com/r/btc/comments/4hfyyo/gavin_can_you_please_detail_all_parts_of_the/d2plygg/

[156] See http://blog.erratasec.com/2016/05/satoshi-how-craig-wrights-deception.html#.WpgiEILLjMW , https://dankaminsky.com/2016/05/03/the-cryptographically-provable-con-man/ illustrating how Wright faked his proofs.

[157] See https://news.ycombinator.com/item?id=11609611

[158] Commit access is the ability to implement protocol changes that only a handful of developers have. Changes to the protocol take two different forms – as either a soft fork that can run despite some nodes still running the old protocol or as a hard fork, which is backwards incompatible.
https://www.reddit.com/r/Bitcoin/comments/4hl7i2/gavins_commit_access_unlikely_to_be_restored/
https://www.reddit.com/r/btc/comments/3wl6sa/can_someone_do_finitely_tell_me_who_exactly_are/
https://github.com/bitcoin/bitcoin/tree/master/doc

blocksize and was one of only two people, the other being the developer Jeff Garzik, that at the time had commit access to the Bitcoin repository. Satoshi Nakamoto themselves had handed Andresen the keys when they left the project and disappeared in 2010, and so discussions circulated about why Andresen (and indeed Matonis of the Bitcoin Foundation) would support the claims of Wright.[159] Because of the timing, in the midst of the scaling conflict, many pointed towards the significance that Wright's claims to being Nakamoto would have in shaping the outcomes of the conflict:

> acqq on May 2, 2016 [-]
>
> > what other reasons could there be for his support?
> >
> > The most obvious reason is simpler: Wright and those who accept his claims are "big-blockians":
> >
> > "Matonis, Andresen and Wright are all big-blockians. Having the esteemed creator Satoshi on their side would help their argument, and it is entirely plausible that there are several large organisations who would benefit from having more control over the regulation of Bitcoin."
> >
> > The same fact is also alluded to in the OP Economist article:
> >
> > "It pays, too, to bear in mind that Mr Wright's outing will most likely be of benefit to those in the current bitcoin civil war who want to expand the blocksize quickly, whose number include Mr Matonis and Mr Andresen. Mr Wright says that if he could reinvent bitcoin, he would program in a steady increase of the blocksize."
> >
> > Add to that that there's this conference in NY today where Andresen repeats his claims: https://vid.me/FhZu
>
> – Forum thread on ycombinator[160]

The conflict continued and became increasingly tense, and in January 2016 Mike Hearn publicly left the Bitcoin project (Hearn, 2016). As discussed above, Bitcoin developers can write code, put forward BIPs and argue their positions but do not finally determine the outcome of the conflict as they rely on miners and full nodes to run any protocol changes, and not long after Hearn's departure over the course of the spring of 2016 it was clear that Bitcoin XT had been largely rejected by the network. The dispute continued with personal accusations, conferences, formal and informal meetings and speculation about the power and interests at stake (Morgan, 2017), while new technical solutions were being worked on by the Core developers. Segregated witness, a technical compromise that had also been presented at the 2015 *Hong Kong Bitcoin Scaling* conference, gained attention over the following two

[159] See Andresen's statement of intentions regarding the maintenance of the Bitcoin reference client after taking over from Satoshi, 2010 https://bitcointalk.org/index.php?topic=2367.0&all=
[160] See https://news.ycombinator.com/item?id=11609611

years resulting in a 'soft fork' with parts of the network running what was called SegWit version of the Bitcoin client. The solution proposed to allow transaction data and signatures to be treated separately. The idea was that this would make nodes accepting 1MB blocks able to validate more transactions by not including signatures, while those nodes accepting and able to compute larger blocks could also do so, essentially allowing small and large blocks without requiring a hard fork (van Wirdum, 2015a, 2015b, 2015c). In the meantime, another version of the protocol, Bitcoin Cash, was launched and mobilised support for a hard fork to increase blocksizes. The name was intended to explicitly reference Nakamoto's whitepaper for Bitcoin as 'electronic cash', and claimed to be closer to that vision by being able to manage more transactions and looking to compete with other online payment systems.[161] The conflict had been going on for some time and a group of users launched a campaign to push for SegWit as a compromise and resolution to avoid hard forks under the Twitter hashtag #UASF.[162] On the 1st of August 2017, those advocating a larger blocksize (including Craig Wright, ex-Bitcoin developer Gavin Andresen, Jihan Wu behind one of the largest mining hardware companies, and vocal Bitcoin libertarians Roger Ver and John McAfee) successfully hard forked Bitcoin Cash.[163] [164]

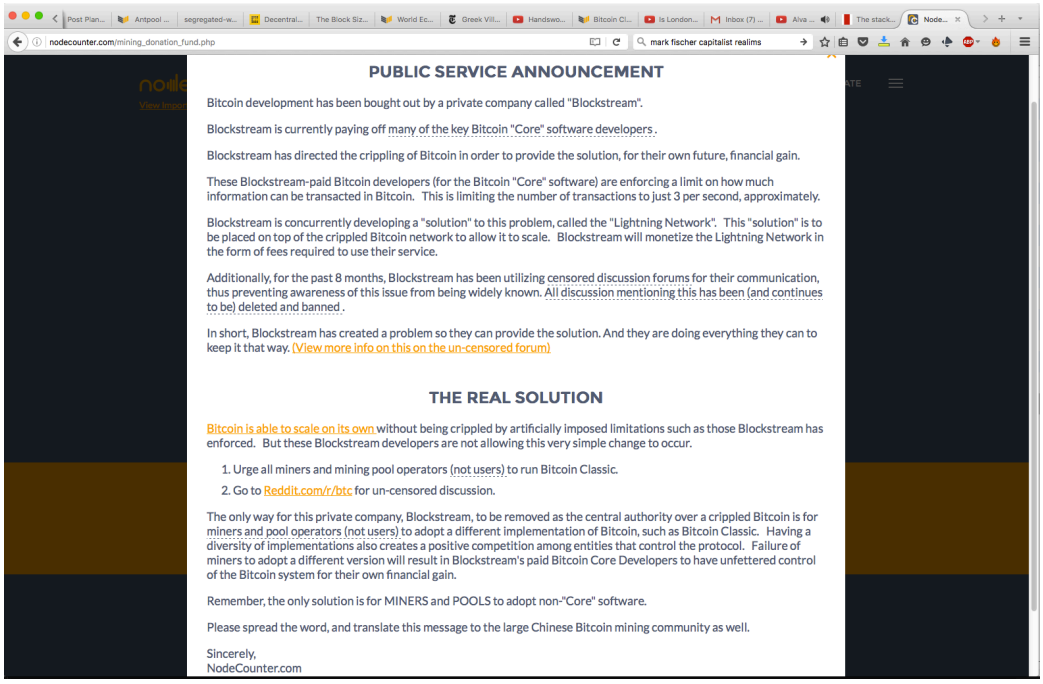

Figure 11. Announcement on the nodecounter.com website illustrating some of the accusations swirling around the Bitcoin community in relation to the scaling conflict.

[161] See for example https://www.bitcoin.com/info/bitcoin-cash-is-bitcoin
[162] See https://transactionfee.info/charts/payments/segwit
[163] GitHub repository: https://github.com/bitcoincashjs/bitcoincashjs
[164] See for example https://blog.sfox.com/the-bitcoin-cash-people-platforms-wallets-and-miners-you-need-to-know-afa53aaa3c66 for an overview.

Through these events, the roles and powers of different kinds of actors were being argued and discussed, and a governance model was being articulated attempting to explain who was or was not in control of Bitcoin (Wirdum, 2016a, 2016b). The scaling conflict and the inability for any fraction to fully 'win' was for some proof of the security properties of decentralisation. In the words of Bitcoin miner Guo, 'people like Bitcoin because it is out of control' (HackerGold, 2016), referring to the fact that no single interest group has been able to take it over and control the protocol, despite what has been interpreted as several attempts to do so. The dismissal of large block solutions, Hearn's earlier departure, Andresen's commit access revocation and the dismissal of Craig Wright as the inventor of Bitcoin were celebrated by some as demonstrating the network's resilience against individual interests and takeover attempts. For others, however, it was a frustrating inability for the network to move forward as well as evidence of the ultimate control by a company called Blockstream based on the fact that several of the Core developers worked with this company (see, for example, the image above). The #UASF by full nodes had in turn been an attempt to resolve the clashing interests of the different camps, but the Cash fork occurred nevertheless, an incompatible differentiation from what then became known as Bitcoin Core resulting in two different and incompatible versions of Bitcoin.

The governance of the Bitcoin protocol had emerged out of open source software development processes for writing, reviewing and deploying code in an open decentralised manner. Relationships and processes outside of the protocol itself were not perceived to matter for the integrity of the technical maintenance. This radically changed in the scaling conflict. 'Decentralisation' was the inviolable principle and measure of legitimacy for everyone involved, but it turned out that the core principle and aim of 'decentralisation' could be interpreted in very different ways; that there were potential trade-offs with other principles and aims; that not all 'nodes' in a network were equal or had similar interests at stake; that they would benefit differently from different solutions; and that what takes place outside of the protocol also potentially matters and cannot be not fully determined through protocological consensus rules. The different kinds of contributors, nodes, exchanges, and affiliations with particular companies, commercial interests and political ideas came to matter and were drawn into considerations and measures of the aim and principle of decentralisation.

6.1.3 Decentralisation politicised

Decentralisation can mean many things to many people and had, from the years 2014 onwards, become a sweeping marketing slogan for the growing blockchain industry more generally. The Bitcoin scaling conflict raised questions around the exact definition and properties of decentralisation in relation to questions of authority and control. Parts of the engineering and developer community sought to establish more precise definitions such that

these could be assessed and measured, maintaining some scientific as well as political integrity of the systems (Srinivasan, 2017; Troncoso *et al.*, 2017; Azouvi, Maller and Meiklejohn, 2018; Gencer *et al.*, 2018; Vorick, 2018). Clear definitions and measurements were necessary in order to assess the state of decentralisation in and for these systems, and indeed to measure whether or not decentralisation was having the intended effects – questions which became particularly important in this period of conflict for the project overall.

As discussed in Chapter 5, decentralisation is operationalised in particular ways for a computer network system, namely in order to solve the problem of authority by making a network that is impossible for any single actor to dominate. But in the scaling conflict new things came to matter for such a condition of 'decentralisation' to be met. The questions of decentralisation and authority were expanded from the state of the network itself and had to be considered in and for the communities writing and maintaining a given protocol, from contributions, comments and discussions on the code base to mining and mining hardware (Srinivasan, 2017; Troncoso *et al.*, 2017; Azouvi, Maller and Meiklejohn, 2018; Gencer *et al.*, 2018; Vorick, 2018). Such studies and attempts at measuring decentralisation are met with the problem of where to draw the limits around what matters and can be determined in and through a description of decentralised governance. For example, measuring 'decentralisation' in the writing of protocols might be done through an analysis of GitHub commits, comments and contributions to the repository (Azouvi, Maller and Meiklejohn, 2018) but this (as the authors themselves point out) does not say much about discussions across other forums and the level of involvement, transparency and engagement at conferences or elsewhere, which equally might affect what gets written and committed to the protocol. The adoption of such changes might in turn be affected by investment in a given piece of mining hardware and the economic interests of the companies involved (Vorick, 2018). The scaling conflict raised the question of what should be considered to matter in the aim of achieving 'decentralisation'.

Modelling and constructing deterministic conditions with certain desired properties are the important tasks of computer engineering and information security disciplines. But the scaling conflict shifted attention from the deterministic relationships in the protocol to the writing, adoption and deployment of the protocol and to all the potential conditions that might affect these – in effect raising a very fundamental question of the limits of what should be considered to matter in the engineering of open, decentralised systems. This question of the limits of the design space is beginning to be understood as one of the particular security and engineering design challenges posed by decentralised open systems (Bonneau *et al.*, 2015; Troncoso *et al.*, 2017). The limits to deterministic conditions might be established in and for a given protocol, but such limits cannot be easily taken for granted in open, decentralised systems and remain an unresolved question in the design and philosophies of such systems. It raises fundamental questions about what aspects of the aims of decentralisation, and its

associated principles, can and should be taken care of through a determinate protocol; and how does the determinate protocol relate to other sensibilities and modes of determinacy, such as the interests of diverse actors in the network (but potentially also extended to other things that might come to matter like geographical, legal and political contexts – for example how these potentially contribute to the concentration of bitcoin mining in China).

An issue with addressing decentralisation as defined and measured only in terms of security is the reduction of the political to a security question. For some, the scaling conflict was a stress test of decentralisation as a security property and systems design resistant to authorities – a test which it passed by resisting the imposition of larger blocksizes, DDoS attacks and takeover attempts by a fake Satoshi Nakamoto. For others, the opposite was the case, and Bitcoin had been taken over by default through clever prevention of blocksize increase by Core developers. But the attraction of decentralised systems, and the motivation for its measure, was not only driven by the notion of authority as a security question, but also around questions of power, and empowerment, freedom, participation and involvement. Decentralisation had been considered an aim in and of itself, with the supposed effects of decentralised architectures remaining vague except for on the question of censorship. This vagueness as to the supposed properties and effects of decentralisation, as discussed in Chapter 5, had been hugely powerful because it allowed people to attach their own expectations of effects onto such decentralised architectures without much scrutiny. The scaling conflict and assessments of decentralisation in and for the processes that the protocol depended on raised the question of what is the definition and meaning of decentralisation beyond the security concerns of the network itself. Other expectations of the effects of decentralisation became important. For example, the issue of authority might be resolved in the network, but does not necessarily address an issue of power more generally; a network without authority can be used very effectively for the concentration of wealth or mining power, for example. And so you can have a decentralised platform and even a decentralised governance structure that nevertheless can be easily manipulated for other purposes that might contradict with other expected effects of decentralisation such as decentralised power, autonomy and so on. The scaling conflict raised these questions not only in terms of concerns about how centralisation of economic interests might affect the security assumptions of decentralised networks, but also in terms of how decentralisation, as a principle and aim, might relate to and in certain designs imply trade-offs with other principles and properties. The most explicit of such trade-offs was expressed in terms of transaction throughput versus protocol decentralisation.

The aim of a given blockchain protocol is to establish determinate conditions and outcomes with particular security properties. As an open, decentralised system, the *dissensible* raised the question of the limits of such modes of determinacy as other sensibilities make

themselves matter in ways that in turn also affect the defined deterministic conditions. Efforts towards defining the supposed properties and measuring the effects of decentralisation are a step forward, where before, decentralisation has been very much considered an aim in and of itself. Such critical assessments are essential for a more grounded assessment of the principle and supposed effects of decentralisation in Bitcoin and blockchain. However, the social and political effects of decentralised architectures remain hugely under-defined and under-examined. There is an important difference and tension between decentralisation as conceptualised in and for network protocols and decentralisation as an ethical, political, social or economic aim or principle that such a protocol might or might not support. Focusing only on one mode of (algorithmic) determinacy in a decentralised, open system is to ignore the ways in which other modes might significantly alter the effects, as would become even more evident over the course of 2016, when in the midst of the Bitcoin scaling conflict Ethereum found itself in its own governance crisis.

6.2 Ethereum and forking as a dissensus mechanism

The Bitcoin scaling conflict brought to light questions of protocol governance. As it turned out, the political could not be fixed in any final manner, even through the consensus mechanisms of a truth machine. This became even more evident in the Ethereum DAO exploit. Ethereum had learned from and replicated aspects of the Bitcoin protocol governance model, for example BIPs, in Ethereum called EIPs, and understandings of the market as part of decentralised protocol governance. Nevertheless, at the height of the Bitcoin conflict in 2016 Ethereum faced its own governance crisis, foregrounding another of the main promises of blockchain as a fix for the political, namely immutability. The immutability of blockchain was important in order for a system to be considered 'trustless' and for the claims of Ethereum as a system operating outside of the control of humans: if the blockchain could be reverted or changed, it implied an authority with such powers, which in turn also potentially undermined the principle of decentralisation, as that authority would need to be trusted. As it turned out, immutability, just as decentralisation, could be determined and enacted in different ways drawing on different modes of determinacy. Protocol governance came to matter for blockchain communities, becoming a major topic of discussions and blog posts and articles (Caffyn, 2015; Hagelstrom, 2016; Wirdum, 2016c; Buterin, 2017; Zamfir, 2018), opening up a negotiation over what might be best determined through a consensus algorithm, when and how 'the social' might be necessary. In the second half of this chapter, I describe a major conflict in Ethereum, namely The DAO exploit, and the ways in which these events forced a rearticulation of ideas of immutable code, governance and determinacy. But first I will describe how 'forking' of code repositories emerged as a *dissensus mechanism* in developer

communities.[165] Forking was, in the Bitcoin conflict, perceived as a negative, as it would split the network, thereby weakening its security properties (by reducing hashrate amongst other things). Through the conflict and more notably in the Ethereum DAO hack, forking began to be reconsidered as part of an accepted repertoire of managing difference and dissensus in ways that correspond to the general sensibility of blockchain, namely an expanded understanding of decentralisation as the possibility for diverse networks, openness and freedom to join or leave a network and repurpose code.

6.2.1 Forking as *dissensus* mechanism

The concept of forking comes out of the open source software community as a way to manage distributed contribution and versioning while ensuring project coherence. Open source software management functions, such as hard and soft forks, pull requests and so on, have through disagreements and conflicts in the blockchain assemblage been politicised and have become understood as governance mechanisms for decentralised protocols without resorting to authorities. Forking in particular has, since the Bitcoin scaling conflict and Ethereum DAO exploit, become a significant aspect of protocol governance. There are several different types of forking with different implications in terms of protocol governance:

Code forks

Code forks came about as a version control mechanism in the coding workflow primarily with the introduction of git and GitHub. Code forks take place all the time and are intended to be temporary, such that a given patch or improvement can be worked on independently and without clogging up or messing with the existing code. The intention is that the patch or improvement will then be merged once it is ready (through a pull request if the author does not have commit access by the project maintainers).

Project fork

Project forks are forks of a given GitHub or git repository with the intention of developing a new project, one that is not necessarily antagonistic but simply builds on what has already been developed. It is a fundamental part of open source culture in which the ability to use what has already been developed (whether code or knowledge more generally) is understood as anyone's right and as a core resource and benefit to everybody because it allows for innovation and development. Plenty of forks were taking place early on in Bitcoin in a creative burst of what are called alt-coins, testing out other designs, consensus protocols and economic or monetary ideas. These forks were not

[165] Forking as dissensus mechanism was a term I articulated with RIAT as part of the *Fork-Politics in Post-Consensus Cryptoeconomic*s at Transmediale, February 2018: https://2018.transmediale.de/content/fork-politics-in-post-consensus-cryptoeconomics

necessarily intended to change or replace Bitcoin as such, but were part of a broader field of experimentation in a period of cryptocurrency development that was characterised by playfulness and curiosity rather than competition. Later forks of Bitcoin, however, have been on the basis of technical disagreements and the relationship between Bitcoin and alt-coins/other blockchain-based projects have become increasingly competitive.

Chain forks

Chain forks are particular to blockchain protocols. Changes to a reference client can force a chain fork and happen when different parts of the network start running different clients. Peers in the network (full nodes and miners) 'witness' transactions that comply with the reference client that they are running. If there is disagreement on the client and the rules it stipulates for transactions, different peers might start to run different versions of the client and nodes might not witness and transmit the transactions they 'disagree' with. In turn, miners might not mine blocks containing transactions that do not comply with what they consider to be the consensus, meaning the chain might split and miners might start mining on different chains.

Soft and hard (chain) forks

There are two types of code and chain forks: hard and soft. Soft forks are changes to a client that are still compatible with an existing protocol and therefore do not necessitate a chain fork. A hard fork entails a fork in the blockchain, meaning nodes need to decide what client they want to run and miners have to decide what chain they want to mine on.

Hard forks were initially not very well received in the blockchain community, partially because they split the network and in the process weaken security; if the network running a given client is smaller, it might be easier for someone to control a large enough part of the network for what is called a 51% attack, namely to be able to dominate the blockchain by controlling most of the mining power. The proof-of-work consensus algorithm organises an emerging consensus that depends on it being impossible for any single node to mine blocks faster than the rest of the network. If the network is small enough, however, it becomes easier for a node or set of nodes to do so, thereby dominating the mining of blocks, and essentially controlling which transactions are verified or not. More recent research, however, has shown that hard forks of both Bitcoin and Ethereum have not significantly split the respective networks; instead, the forks have generally drawn in new contributors (Azouvi, Maller and Meiklejohn, 2018), with new constituencies formed around and mobilised by new visions for Bitcoin and Ethereum.

The idea of forking expanded on the notion of the digital as making possible a different kind of politics whereby rules and realities are complied with in a voluntary manner and new rules, new realities, relations, currencies and constituencies might be created as and when needed. Such notions of forking tend to exclude the ways in which such rules and constituencies depend on much more arduous contexts and relations that nevertheless remain the same regardless of which new client is run (see Chapter 5). Through Ethereum's own governance crisis, new articulations of forking began to form as a dissensus mechanism, and these were perceived as a powerful tool for forcing a 'vote' on protocol changes by forcing the network to chose which client to run, drawing human decision-making back into the system but without resorting to authorities. For others, however, forking also represented a betrayal of the promise of immutable code and non-algorithmic determination, representing the return of authorities.

6.2.2 The Ethereum DAO exploit

Ethereum was a project to generalise the Bitcoin blockchain such that instead of only transactions, the blockchain would also hold bits of code and execute any type of computation. These bits of code were articulated as Smart Contracts – contracts that would execute as written, and beyond the control of any person or institution once they had been deployed because the contracts would be held in a decentralised manner and executed on the basis of financial incentives. A cluster of such Smart Contracts was then envisioned to form a Decentralised Autonomous Organisation (DAO), an organisation that would operate on and through a decentralised network, beyond the control of humans, beholden only to its contract code. The first explicit instance of a DAO was developed and launched by the Ethereum-based Internet-of-Things company Slock.it in the spring of 2016.[166] Its purpose was to act as a fund to invest in Ethereum-based start-ups, motivated by a desire to expand the decentralised model to the actual funding of new projects rather than be reliant on venture capital funding and traditional business models. The creators of The DAO promised an entirely new organisational model that would be governed only and explicitly through its contract code (Tual, 2016a, 2016b, 2016c) independent from any legislation or human intervention. This was emphasised and enshrined in a document where it was made explicit that any statements of intent, publications or promotional material would have no implications in the running of The DAO. The contract code, and only the contract code, would count in its governance:

> The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or

[166] See https://daohub.org/

> guarantees beyond those set forth in The DAO's code. Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supercede or modify the express terms of The DAO's code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of The DAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, **The DAO's code controls and sets forth all terms of The DAO Creation**.
>
> – Terms set out on The DAO website, 2016[167]

On the back of the attention surrounding Smart Contracts and Ethereum as a whole, The DAO received near $22 million worth of ether in the first week of token sales, much more than was anticipated.[168] [169] Over the next months the value of The DAO soared to over $100mil. The intention was that start-ups would submit proposals for new Ethereum-based projects and applications, which The DAO would then fund after a round of voting by token holders. Slock.it themselves submitted a *proposal 1*, in which they suggested an Ethereum 'network of things' sharing platform (Slock.it, 2016) in which The DAO would receive a percentage of any revenue generated in the platform, providing a return on investment to token holders.[170] There was no time for more proposals to be submitted, however, because on the morning of the 17th of June 2016 the funds in The DAO contract account started to drop substantially; an amount of 258 ether tokens were being repeatedly sent to a new DAO address rapidly emptying The DAO of funds totalling approximately $60 million worth of ether.[171] The hack turned out to be a combination of functionality in the code, in which the `splitDAO` function that automatically releases a token holder's initial investment, the very function that is supposed to protect token holders from attacks by allowing them to withdraw their funds in case they, for example, disagree with curator, was being looped, sending funds to a new `childDAO`.[172] As news began to spread, the value of ether crashed. Because the amount of investment siphoned off to the new DAO represented a large market share of the ether currency, it became a problem not only for the Slock.it start-up but for the Ethereum platform as a whole, forcing interventions and statements by Ethereum core developers (Buterin, 2016b). In some frantic hours in which exchanges were asked to shut down all trade in ether to prevent the hacker from withdrawing the tokens and exchanging them to fiat currency, thoughts of 'rolling back'

---

[167] See https://web.archive.org/web/20160501124801/https://daohub.org/explainer.html (accessed June 29th 2016) This quote was circulated across forums, articles and blog posts commenting on the exploit, the likely or best response and rights of investors, etc. See also a supposed letter from the hacker/exploiter https://pastebin.com/CcGUBgDG

[168] See https://blog.slock.it/the-inexorable-rise-of-the-dao-2b6e739b2615#.f1gaowogr

[169] Ethereum developer Vlad Zamfir stated in conversation that the amount of investment in The DAO far exceeded anyone's expectations, and probably exacerbated the security risk.

[170] The principle of disintermediation seems to have given way to a more traditional corporate network '*rentier*' model, the innovation instead being in the ease at which ownership and stakes can be traded, and the management of funds by cryptographically enforced agreements.

[171] The address showing all the transactions can be browsed here: https://etherchain.org/account/0x304a554a310c7e546dfe434669c62820b7d83490#txreceived

[172] http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/

the blockchain were floated. Ethereum founder Buterin issued a statement suggesting a soft fork, which was dismissed on the basis of further security issues.[173] Founder of the company Slock.it Tual pushed for a hard fork in which the split would be reversed and all funds would be returned to token holders.[174] The idea of a rollback or a fork was met with furious response by exchanges and parts of the community. The comment below was symptomatic in many discussion forums following the fork proposals:

> The "too big to fail" approach is what the crypto-world set out to solve in the first place, now one of the chief projects is flat out admitting that "too big to fail" is an ok policy.
>
> – User “Ledgers” on reddit discussion[175]

The very purpose of Ethereum, a platform promising unstoppable decentralised applications and Decentralised Autonomous Organisations, was being betrayed. Code that was supposed to be beyond the reach of control and thereby beyond any potential political disputes or censorship turned out to not be so easily extracted from human concerns. A leaked chat between some of the Ethereum core developers and cryptocurrency exchanges in the early hours of the exploit show the resistance to a rollback as a serious violation of the ‘immutability’ of the blockchain and Smart Contracts.[176] The DAO had, after all, been advertised as being governed only and exclusively by the contract code – which in this instance indeed allowed for calling the `split` function in a loop. A rollback of the blockchain (restarting the network from a block before the exploit had taken place) through a decision by the core developers was seen as undermining the promise of immutability and the whole purpose of trustless system:

> [4:59:49 AM] QIU Liang: YUNBI Exchange think ROLLBACK IS EVIL
>
> [5:00:01 AM] Mike Li: We don’t agree rollback
>
> [5:00:35 AM] Craig Sellars: You can't claim immutability and then change the ledger.
>
> [5:01:05 AM] Mike Li: Rollback will be unfair for all ETH traders on Yunbi
>
> [5:01:14 AM] Philip G. Potter: even a serious discussion about a rollback by eth overlords IS EVIL
>
> – Chat-log between Ethereum developers and exchanges, June 18th 2016[177]

[173] https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/
[174] https://blog.slock.it/a-fork-in-the-road-c3c267b9ff31#.1ubf6r5x0
[175] https://www.reddit.com/r/ethereum/comments/4oj7ql/personal_statement_regarding_the_fork/
[176] See also https://medium.com/swarmfund/daos-hacks-and-the-law-eb6a33808e3e that assumed the exploit would have to be honoured.
[177] See http://dpaste.com/1SH9EQA.txt and also https://bitcointalk.org/index.php?topic=1139044.msg15261584 and responses here: https://news.ycombinator.com/item?id=11921900 and https://medium.com/@iconomi.net/ethereum-thedao-it-is-about-what-you-believe-in-2116d1f4ce88

Eventually, a hard fork was developed by the Ethereum Foundation in order to recover investors' funds. The hard fork would move the hacker's funds from the `childDAO` into a new contract account with only one functionality, namely to allow token holders to withdraw their original investments of ether. Because such a fork would rollback on a function that was in fact permitted in the contract code, there was another round of strong negative reactions in online discussions, seeing a fork as a fundamental breach of the stated intent of The DAO in the first place. The blockchain and Ethereum contracts were supposed to be immutable, beyond interference by any human, and the main promise of The DAO was that it is entirely governed by its contract code. The 'hack', it was argued, was in fact permitted according to The DAO contract code and so should not be considered a hack but an 'exploit' of existing functionality. Not long after, a letter was published addressed to The DAO and Ethereum communities claiming to be from the person behind the hack:

> I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting is rewarded with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank The DAO for this reward. It is my understanding that The DAO code contains this feature to promote decentralisation and encourage the creation of "child DAOs".
>
> I am disappointed by those who are characterising the use of this intentional feature as "theft". I am making use of this explicitly coded feature as per the smart contract terms and my law firm has advised me that my action is fully compliant with United States criminal and tort law. For reference please review the terms of The DAO.
>
> – 'An open letter to The DAO and Ethereum community'[178]

While there were doubts as to whether or not this letter genuinely came from The DAO hacker, the points raised in it were circulated and became a focus of debate. The DAO exploit and following hard fork pushed the community into a flurry of discussions and proclamations on the relationship between technology and the social world in a search for coherent explanations and justifications for or against the hard fork. In the week leading up to the hard fork, a 'crypto-decentralist manifesto' was published reminding the Ethereum Foundation, core developers and Slock.it of earlier claims of decentralisation founded on principles of openness, immutability and neutrality.[179]

The hard fork was announced to take place at block 1920,000, estimated for the 21st of July 2016. The day would prove whether or not there was 'consensus' for the fork, meaning

[178] See https://pastebin.com/CcGUBgDG Also, there was some discussion whether the letter was indeed from the hackers or not, but also general agreement that it hardly mattered because the discussions sparked by it were relevant more broadly, see https://news.ycombinator.com/item?id=11927891
[179] https://medium.com/@bit_novosti/a-crypto-decentralist-manifesto-6ba1fa0b9ede

whether miners would adopt the changes and begin mining on the new chain. The http://fork.ethstats.net/ website was set up to monitor which blockchain miners were mining on and relatively quickly it became clear that there was broad adoption. The hard fork by the Ethereum Foundation was successful but only a few days after, headlines appeared about Ethereum Classic – an initiative to keep mining on the original Ethereum blockchain, a chain and version of events in which the exploit was not reverted.[180] After one of the main exchanges (Poloniex) declared that they would facilitate trade in Ethereum Classic tokens the value went up and miners began to declare their interest.[181] The statement on the Ethereum Classic GitHub site states the motivations behind the continued mining explicitly:

> We believe in decentralised, censorship-resistant, permissionless blockchains. We believe in the original vision of Ethereum as a world computer you can't shut down, running irreversible smart contracts. We believe in a strong separation of concerns, where system forks are only possible in order to correct actual platform bugs, not to bail out failed contracts and special interests. We believe in censorship-resistant platform that can be actually trusted - by anyone.
>
> – Ethereum Classic GitHub repository, 2016[182]

Ethereum Classic and the old chain of events proved successful and is, as of writing, still actively mined on and used – meaning there are now two versions of Ethereum, two versions of history: one where the exploit was reverted, never happened and investors still have their ether, and one where it did happen and investors lost their ether to the childDAO. For the rest of the network using Ethereum, a chain fork essentially means a duplication of accounts, meaning those who held their own keys to their ether wallets gained an equivalent of ether classic tokens.

Soon after, Ethereum Classic publicly gained the support of previous Ethereum founder Charles Hoskinson (Rivlin, 2016) who had left the Ethereum Foundation in 2014 due to disagreements over the governance of Ethereum. Hoskinson had, since departing from the Ethereum Foundation, launched the company IOHK (Input Output Hong Kong)[183] and a new Smart Contract platform called Cardano, with a cryptocurrency called ADA coin.[184] They raised investment specifically in Japan, with promise to launch their blockchain in early 2017, but still have not built or launched their blockchain, and according to a blogpost from Ethereum Classic stopped communication with investors (Ethereum Classic, 2017). This raised questions about why the coin had only been marketed in Japan, whether this was to prevent scrutiny from the rest of the cryptocurrency community, and brought accusations that

[180] http://www.coindesk.com/ethereum-hard-fork-creates-competing-currencies-support-ethereum-classic-rises/
[181] https://poloniex.com/exchange#btc_etc
[182] See https://ethereumclassic.github.io/
[183] See https://iohk.io/
[184] See https://www.cardano.org/en/home/

the project was a scam.[185] A blogpost in May 2017 suggested that Hoskinson's involvement in Ethereum Classic looked suspiciously like an attempted takeover of their protocol governance, having shifted attention from Cardano Smart Contract platform after the promised date of the ADA coin launch had passed (Classic, 2017). As of writing, Hoskinson is still promoting Cardano and ADA coin as a 'third generation blockchain' but IOHK have not yet launched their blockchain.[186]

Such disputes, rumours and scams had at this point become rife in cryptocurrency communities, as the hype of the technology had reached a peak and investments were easy to come by. The difference and contradiction between the claims of blockchain systems as trustless and beyond corruptibility and the number of fake projects and unfulfilled promises became glaring as governance crises rippled throughout most projects, followed by legal clampdowns, in particular in relation to Initial Coin Offerings. In a sense, two contradictory governance descriptions coexist: on the one hand, the claim that decentralised systems exist beyond both corruptibility of humans and the reach of existing regulatory authorities, and on the other, the reality that most blockchain projects do incorporate as companies and foundations in order to be able to operate legitimately, for example in order to have their tokens listed on the large exchanges, and have in many cases have relied on existing legal frameworks. The intersection of the two conditions are rarely explicitly mapped out, dealt with and designed for in discussions of decentralised governance, possibly because of a belief that the decentralised models will eventually 'escape' the bind of existing legal frameworks once built and fully functional. Regardless, this actual intersection and strategic navigating between existing legal frameworks and processes, and the governance thinking and theories coming out of the blockchain space in relation to open decentralised governance structures, would benefit from further research, in particular in relation and comparison to research done around attempts to regulate, tax and hold accountable large transnational technology, to see where and how blockchain companies and foundations seek to differentiate or not in relation to these. The particulars of blockchain protocol governance are worth outlining, as has been the ambition above, but they do not address some important areas, such as the ways in which protocol governance and attempts at decentralise these intersect and are affected by legal incorporation as companies and foundations, and the associated governance methods and processes entailed, in turn affect, intersect with and contradict these decentralised aspects. To state it more explicitly, liability cases and the pressures of existing legal frameworks mean that specific names need to be on documents, and people and assets are at stake, in turn also determining a service relationship with users or customers – all of which are not entirely compatible with ideas of open, decentralised and autonomous systems.

[185] See https://twitter.com/AceOfWallStreet/status/841743375346851842 and https://twitter.com/CollinCrypto/status/841770372764733442 for Hoskinson's comments in the Ethereum Classic Slack channel about the tweet.
[186] See https://ethereumworldnews.com/charles-hoskinson-cardano-trillion-dollar/

So far I have recounted how the DAO exploit forced a reassessment of some of the main promises of the Ethereum platform, namely to be a platform for code, contracts and organisational form that would be beyond reach of any authority, determined by and running solely according to the stated contract code. As it turned out, the political could not be fixed in any final manner, code was not simply neutral and the blockchain was not immutable. In the following section I discuss some of the ways in which these events caused a rearticulation of the remit of blockchain and the Ethereum platform in particular, explicitly integrating 'the social' into processes for determining consensus at a protocol governance layer.

6.2.3 Integrating social consensus

The Ethereum DAO exploit severely challenged the idea of developing systems that would operate beyond the control of humans and in a realm of mathematical, predictable and transparent execution. Instead, the execution of code turned out to be less than predictable and certain. These events diffracted the principle of immutability with new articulations, on the one hand arguing 'only social consensus trumps code' (see tweet below) and on the other that the Ethereum social contract had been breached in the fork (see above, and Rivlin 2016). Decentralised systems now began to include some notion of human and social determination through an 'implicit' social contract amongst the community (Zamfir, 2016).

Figure 12. d11e9 retweets Ethereum developer Vlad Zamfir's celebration of the hardfork, July 2016.

Discussions around social or technical determination have since evolved into questions of on- or off-chain governance (Ehrsam, 2017; Zamfir, 2017; Buterin, 2018; Kreutler, 2018) in efforts to solve the political through new technical means or refuting such efforts by acknowledging the political. The changing attitudes towards some of the main design and political principles are captured in the table below.

	Ethereum pre-exploit	Ethereum hard fork	Ethereum Classic
Immutability	Blockchain is immutable.	The blockchain is immutable but can be changed through community consensus.	Blockchain must remain immutable.
Decentralisation	Ethereum is a project to take decentralisation to the next level and counter the centralising tendencies of Bitcoin.	The hard fork would not have happened if there was no consensus to implement it, therefore decentralisation has not been compromised.	The hard fork represented some people's interests over others and therefore compromises some aspects of decentralisation.
Community	Anyone in the Ethereum ecosystem. (Seems to only be a word that is mobilised when some form of legitimacy is called upon 'what the community has expressed', 'what the community wants' 'the community wins again').	Loosely consists of users, miners, businesses, blockchain media, commentators, developers, and the foundation, but no precise understanding of who the community is or how power dynamics operate in this space.	The community is what mobilises against centralising tendencies.
Authority	Authority is guaranteed distributed by the immutability of the code.	'The community', clients and social consensus have the ultimate authority.	The authenticity of the code must remain the only authority. If not, otherwise the system is biased.
Governance	The community is self-governed through market incentives and secure immutable code.	Hard forks are just another governance mechanism for the community.	The system is self-governing through immutable code founded on decentralisation, openness and neutrality.
Calculation (and indeterminacy)	By incorporating rewards and punishment all behaviour can be calculated, accounted for and managed in a decentralised manner.	When the unpredictable happens, the community will decide what is the most just want of calculating. (Ethereum still a project of expanding the realm of calculation.)	While all events might not be calculable, the rules must remain the same for everyone and should not be changed, even and especially if that means someone loses out as that would favour special interests over neutrality.
Neutrality	Code is neutral as opposed to vague human language.	The community has values, which should be respected and enforced through consensus.	Distinction between 'bugs' that should be fixed, and special interests, which should never affect the code.

Table 4: changing attitudes to principles in Ethereum over the DAO exploit.

Discussions and debates on reddit, Twitter and elsewhere about The DAO exploit were at times vitriolic and very tense. But although there were harsh words written about the different implementations, forking is an integral and accepted practice and so there was also quickly an acceptance of the Ethereum Classic project, and efforts from developers on all sides moved on to focus on the potential security issues of having two chains. A comment by Smithgift in October 2016 expresses worry about future incompatibility between the two chains. They describe a 'metaethereal' world, expressing a continued desire for interoperability between chains and ensuring it is usable as a platform down the line for applications that want to function across chains:

> …In any case, the existence of two incompatible replay protection systems will hardly cause them to fail in their intended function. It's just a kind of balkanisation of code that, IMHO, would be harmful for a future cross-chain metaetheral world. I'm not saying that doing our own system would be wrong, but that there's a non-zero cost to having different systems.
>
> – Discussion on the Ethereum Classic GitHub repository[187]

Such concerns for a higher level of interoperability shows the extent to which forking at this point had become an acceptable way to express dissensus and exercise freedom to determine one's own protocol while still considering a common project at a 'meta' level. In the case of the Ethereum DAO hard fork, in particular developer Vlad Zamfir, who had been involved in the writing of the Ethereum fork, engaged in a rearticulation of hard forks as important and useful tools for decentralised governance as it allows for 'social consensus' to intervene and decide and prevent potential negative uses of a system (see *Fig. 14* above and Zamfir 2016).[188] For one of the people behind The DAO, Stephan Tual, not only that, but that 'Hard forks are the most democratic means of consensus on earth today. They are the ultimate referendum mechanism' (Tual, 2016d). This was a significant shift in the discourse surrounding governance that previously had been addressed as a problem to be removed from human interference and resolved through algorithmic means (see 4.2.1). The role of 'the social' and the ability for actors to organise outside of the system in order to mobilise consensus started to be integrated into the ideas of how governance in these new decentralised systems operate.

Acknowledging the social, however, does not entail organising it. Zamfir and much of the blockchain community remain anti-institutional and are not keen on formalising social consensus processes. Institutions are understood as too rigid, oppressive and 'easy to game'

[187] See https://github.com/ethereum/EIPs/issues/155
[188] In Zamfir's opinion the whole DAO project had been rushed through. He had co-written a moratorium (http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/) after finding many issues that could be 'gamed' in the code but not much had been done to correct these. In his opinion the hack was a lesson on the importance of getting the code right in smart contracts and the role of social consensus more broadly.

as opposed to decentralised computational systems that are secure and have transparent rules that people can engage with or disengage from as and when and to the extent that they want to. The idea is that 'split' functions and hard forks are safeguards against the systems becoming oppressive; if you disagree with the direction of a project, simply fork the chain (or indeed split The DAO).[189] However, both the Bitcoin scaling conflict and the Ethereum DAO exploit show that in order to successfully fork, a network requires significant capacity beyond the protocol changes themselves, which looks a lot like lobbying, campaigning and other practices from what might be considered traditional politics, in order to get enough people and machines to form a functioning network. Peer-to-peer networks also imply network effects that can make it significantly difficult for some actors to fork in any effective manner. The involvement of 'the social' in determining aspects of the protocol in this sense was and still to a large degree remains under-examined, outside of immediate engagement with the protocol itself. For example, miners and core developers are much more coordinated and have much more established methods of communication than the loose network of end-users, the multiple actors running clients and using the platforms. Governance is instead addressed primarily in direct relation to the protocols and platforms. The project to develop protocols, applications and apparatuses that are independent from any specific human, that anyone could join, leave, contribute to or fork continues across disagreements.

The Ethereum project, as a project to generalise the consensus algorithm of Bitcoin, had turned the Bitcoin solution to double-spending into a generalised solution to governance (see Chapter 5). In the process, the political had been turned into a security concern, which has been addressed and solved as a systems engineering problem, such that undesirable behaviour would be eliminated through the right combinations of incentives and cryptography. 'Malicious behaviour' would thereby be made either impossible or undesirable enough that it would not occur. The DAO exploit, however, forced the question of who gets to determine what is 'good' or 'bad' in the first place, whether what happened with The DAO was a hack to be corrected for or an exploit to be applauded. In her analysis of the post-political in the context of European liberalism, political theorist Mouffe argues that dissensus of the kind that threatens the foundations of liberal ideas and institutions is marginalised to such an extent that it is no longer considered a legitimate political position, but a moral one of 'right' and 'wrong', 'good' and 'bad' (Mouffe, 2005). In and through the scaling conflict and The DAO hack, two different responses seem to emerge. In some cases, the political in the sense of dissensus with the very conditions of governance protocols is turned into a security question. The manner of dealing with 'malicious' versus 'honest' behaviour is one way in which

[189] Forking, as an approach and method emerging out of open source software development, also relates to ideas of meritocracy in which people with the skills and abilities to improve on something should be able to freely do so. Some of these ideas have a more explicitly ideological articulation in a US anarcho-capitalist tendency called *voluntarysm* that amongst others Bitcoin and libertarian Roger Ver subscribes to. It is a market-based form of anarchism that however is strongly anti-corporate as it is against monopolies and any state involvement. Corporations are seen to collaborate with the state to oppress people's freedoms.

dissensus is shifted from a political question (with the open debates around what should or should not be considered malicious behaviour) to a security question (malicious behaviour should be made impossible). The other response was one that indeed recognised the political as a right to difference and differentiation. This was largely resolved through the notion of forking such that difference could be recognised and accommodated for. Continued interoperability between different forks then emerged as the next task, with new projects seeking ever more 'meta' layers in order to facilitate such interoperability. In the case of the Ethereum DAO exploit, the opposite occurred, and what had up until then been treated as self-evidently good or bad, malicious or honest behaviour in the network became politicised. The Ethereum DAO exploit and subsequent fork had brought 'the social' into focus as a potentially valid process for determining changes to the protocol. The promise of immutable code and systems beyond the control of humans was shown to be a promise and project rather than an inevitable state of things emerging out of the nature of cryptography and decentralised networks. The fork was, at essence, about this very question, the extent to which social determination should be allowed in relation to the protocol. The Ethereum foundation and developers had made a decision on what was in the best interest for investors, the community and the project, which was accepted and enacted by a large part of the network running Ethereum; in the meantime Ethereum Classic sought to maintain the initial promise of immutable code and refused intervention from anything outside of the existing rules of the code gathering a constituency around this understanding.

Such questions, of who or what should determine the protocol, were expanded to include protocol governance and discussions continued in the form of on-chain or off-chain governance processes. Off-chain governance, argued for by amongst others Zamfir, to some extent acknowledges the political as an ongoing negotiation, describing an 'ever-changing social contract' (Ehrsam, 2017; Zamfir, 2017) (while the ways in which such an ever-changing social contract is articulated and negotiated remains under-explored). The argument for an expansion of algorithmic determinacy was, curiously, also argued for exactly on the basis of accommodating different sensibilities. The author(s) of the crypto-decentralist manifesto discussed the question of different sensibilities in relation to the social, but the social was here challenged in terms of the extent to which 'social' sensibilities understood as human could accommodate for the non-human sensibilities of artificial agents including these as part of a 'wider set of constituencies' that blockchain systems would serve:

> I believe that "blockchain tech" is in fact a social technology. Community consensus is an integral part of "blockchain tech" same as cryptography, network protocols and consensus layer. However, I feel that focusing on "human participants" is shortsighted since blockchain systems will come to serve a much wider set of constituencies, including artificial agents that may not necessarily share our sensibilities. Serving as a dependable, predictable and

> frictionless mechanism for economic and social cooperation between entities of all sorts. So, basic blockchain characteristics and rules of the game should be simple and understandable for everyone. Not dependant on social instincts and judgements of intelligent primates. It won't be fair to other participants, which therefore won't participate. So neither human nor "refrigerator judgement" should be necessary as part of the system.
>
> – Bit Novosti, July 2016[190]

The conclusion drawn from acknowledging the diversity of sensibilities was that 'neither human nor 'refrigerator judgement' should be necessary as part of the system'. Differences in sensibilities were sought overcome, once again, through the pursuit of a neutral substrate of 'dependable, predictable and frictionless mechanisms' that could take place between supposedly any human or artificial agent. Such approaches have given rise to the idea of on-chain governance, whereby blockchain mechanisms would also be brought in to determine protocol governance.

Given the ontological effects of the sensing apparatus, inclusion into a given sensibility can have effects of eliminating and excluding other sensibilities as mattering. Already existing difference might not register on a given sensing apparatus. This is, in fact, the very purpose of a deterministic system like blockchain: to ensure that differences are settled and determined in a 'frictionless' manner. In the case of blockchain applications, this might be the relations, transactions or otherwise that do not take place via the protocol – or, in the example of the economic apparatus of price mechanisms, this would be all the 'stuff' that does not enter into market relations. The ways in which determinate systems engage with other sensibilities and other modes of determinacy is foregrounded as mattering here and through The DAO exploit. The acknowledgement and recognition of the necessary particularity of a given mode and medium of governance, and its ontological effects, should be cause for hesitation in terms of immediate inclusion of any new sensibility that makes itself felt, and for efforts to be made in understanding such effects while also looking at other possible sensibilities – for example the beginnings of an acknowledgement of 'the social' as a mode of determination in relation to blockchain governance.

The DAO exploit and subsequent negotiations over the involvement of 'the social' are nothing less than the negotiation over which sensibilities are appropriate for determining different aspects and processes around the legal, economic and social intra-actions, their limits and how these sensibilities and modes of determinacy relate to one another. The political signification of that relational space is hugely under-studied in the development of new blockchain applications, most likely because of the particular practices of engineering and

[190] See https://medium.com/@bit_novosti/i-believe-that-blockchain-tech-is-in-fact-a-social-technology-6d409fa6e97e

information security, examining and developing determinate conditions. There are, however, developments in this relational space, and from the information security field itself (Zurko and Simon, 1996; Rogaway, 2015). Broadening the information security and privacy design considerations from the systems themselves to focus on the interactions with users, there is an acknowledgment that information security cannot be addressed in a meaningful way without taking into account the way security plays out in practice. In terms of design strategy, what this means is that the concern cannot only be the construction of determinate conditions meeting specific security requirements and design principles (decentralisation, immutability, etc.) in and of themselves. The concern has to be what is determined in and through the relation between the constructed determinate conditions of a blockchain protocol and the ways it meets the *otherwise* determined (socially or culturally, as discussed above), as well as the indeterminate, potentials for incompatible differentiation to emerge.

Consensus protocols and also protocol governance (as dissensus protocols), whether off-chain or on-chain, do not 'fix' the political in any final manner, but are particular forms and mediums for managing dissensus and the dissensible. These forms and mediums matter politically (and, in turn, can be contested). Fixed notions of mediation, whether based on the certainty of universal values, mathematical laws, price mechanisms, largest voting numbers, or fairest institution, when understood as universal, flatten the registers of what matters and how things come to matter (Yusoff, 2013a). The lessons here are therefore threefold: the political cannot be fixed in any final manner; the particular mediums through which to negotiate and settle differences matter in and of themselves and can therefore be contested; there are many potential sensibilities and these therefore demand attention to the relationships between these and a certain spaciousness to be determined through other sensing apparatuses in the Baradian onto-epistemological sense (Barad, 2007, pp. 132–186).

6.3 Conclusions

In response to the scaling conflict, attention shifted from the protocol itself to its governance, measuring and applying the principle of decentralisation at this layer. Addressing the dissensible as a governance problem tempts further efforts towards resolving and fixing the political with more decentralisation, to ensure that no single authority will dominate. In this sense it seems to present a problem of infinite regression, seeking to measure and apply a decentralisation 'fix' at ever-deeper layers as and when dissensus emerges. Any attempt at measuring decentralisation necessarily requires a clear definition of what is being measured. Drawing in Barad and Rancière, such definition and subsequent measuring in turn determines the characteristics of a necessarily particular instance of 'decentralisation' in an onto-

epistemological manner, to the exclusion of other potential materialisations of the notion. This particular instantiation of decentralised systems in turn might be contested if and when different and potentially incompatible articulations of decentralisation are made to matter.

This can be explained by discussing some more implications of and expanding on the definitions of the political that have been built through the previous two chapters, namely as a *disruption to what is sensed as mattering by a given apparatus*. Blockchain technologies sought to disrupt existing methods of resolving differences, namely legal and political processes, looking to shift the sensibility around who or what should be able to intermediate to include (or in the case of maximalists, solely comprise of) algorithmic processes. This in itself then becomes a new sensibility, a new sensing apparatus, and a potential site for dissensus, a different sensibility to emerge. Through this understanding, then, the political is never fixed or resolved; it is simply reconfigured into different forms and mediums – and these new forms and mediums might in themselves become politically contested. This inability to finally 'fix' the political does not mean that establishing new governance mechanisms, new ways of doing politics, is futile or meaningless. On the contrary, and returning to Barad and the ontological effects of apparatuses, such new mediums matter, literally. The apparatus, through which the management of difference takes place, matters, in the sense that it will always be particular. They make a material difference in ways that should be ethically and political scrutinised and never assumed as universal or final.

Decentralised technologies in a sense represent one particular resolution to *the political* materialised in and through collaborations with non-human phenomena to form new apparatuses of governance. These might have desirable or undesirable effects, and should each be analysed accordingly. Some actors will be more able than others to navigate particular methods (the legal system, or a code repository, BIP process, forking, etc.), while others might in turn seek to disrupt this method and establish different mediums for navigating and resolving differences. Any description, encoding or understanding of what is sensible will always entail acknowledged or unacknowledged exclusions of other positions, perspectives and sensibilities, and thereby will also entail the possibility that these will make themselves felt, and disrupt a given sensibility. But the particulars of the mediums for resolving differences and incompatibility matter, exactly *because* they are never neutral and never universal and therefore have particular material effects. To make this clearer, instead of understanding blockchain and blockchain governance as a wholesale replacement of existing political, legal and governance institutions, and therefore having to address any potential issue to do with decentralisation and power, it would be more fruitful to assess blockchain governance in terms of a much more contextualised understanding of what the technology might be able to do. Referring back to discussions in 5.1, this might be, for example, as a network space that operates beyond control of existing political and financial authorities, in

the context of geo-political stakes in internet protocols. In other words, I want to suggest a contextualised discussion on the political purpose of blockchain protocols in relation to current systems, and what might be the appropriate governance mechanisms for these.

In this chapter I have therefore distinguished between governance and the political. Where blockchain protocols are intended to replace authorities through a decentralised network that mediates and organises consensus, dissensus might arise as to the actual development of the protocols themselves. These disagreements also brought out different interpretations of core principles and claims of blockchain, forcing new articulations of these principles that would include 'the social' in their realisation. Stopping short of the political, however, the issue of dissensus has been largely either addressed through notions of encoding new 'on-chain' governance processes, or by seeking determination in an under-defined realm of the 'social'. On-chain governance processes open up an issue of infinite regression whereby the question of how to resolve dissensus is met with a decentralisation fix at ever higher or deeper layers. It is helpful to instead distinguish between governance, as particular modes of managing difference, and *the political* as an ongoing *potential* for dissensus and something new to make itself matter. I discuss three consequences of this distinction in relation to blockchain governance. Firstly, the political is not something to be solved in any final manner and that any claim to do so entails repression or ignorance towards difference. Secondly, specific instances and mediums of resolving the political nevertheless matter (in fact matter more); as became evident through the conflicts, the very protocols for resolving and mediating difference also became an area of disagreement and differentiation, not only of opinion but also of determination. The mediums have ontological effects, which also demand recognition of multiple modes of determination (including 'the social' and countless others). Thirdly, the recognition of different forms of mediation, determined through other sensibilities of what matters (such as the social), points attention towards how these are related to. Rather than solving a given problem of difference internally in a deterministic protocol, the relationship between a given protocol and other sensibilities can start to be considered and be placed in the foreground in terms of design and engineering.

The acknowledgement that there are many things, relations and situations that cannot be determined and fixed through the protocol has begun to open up a space for acknowledging and analysing what happens outside and around blockchain systems and protocols. *The political* goes directly against the idea that it is possible to finally fix questions of power, both in the sense of fixing a problem, and fixing as determining a fixed, dependable and provable condition, exactly because what matters can never be finally known or fully modelled but instead should be considered as an ongoing and at times contested field of (indeterminate) potential. Consensus protocols and also protocol governance (as dissensus protocols), whether off-chain or on-chain do not 'fix' the political in any final manner, but are particular

forms and mediums for managing the political. These forms and mediums matter politically (and, in turn, can be contested). Fixed notions of mediation, whether based on the certainty of some universal values, mathematical laws, price mechanisms, largest voting numbers or fairest institution, when understood as universal, flatten the registers of what matters and how things come to matter (Yusoff, 2013a).

7 Conclusion: reassembling the trust machine

With this thesis I have sought to answer the question of what matters politically in blockchain. When I began my research, it quickly became clear that the technology was attracting attention and efforts from a wide variety of contexts, geographies, political/economic tendencies and industries. The motivation for, and intention of, asking this question was to understand this broad attraction, to seek out which aspects of blockchain might determine its political effects, to analyse its possible implications and how these implications might be made differently. The thesis overall then is intended to contribute to a growing body of critical literature on blockchain technology. Situating blockchain in debates on the politics and ethics of algorithmic mediation, digital platforms and platform economics and questions of governance and political theory in the context of planetary scale computation the thesis is an assessment of its potential implications and claims made of it and in turn contributing to related literature. As the research progressed, I have increasingly taken the position of critical insider in the field, collaborating with developers and computer scientists, with an aim of also contributing to technical and industry debates, highlighting issues in blockchain protocol and governance design. The main aim of this thesis has therefore increasingly become not only to assess, but also to actively situate the technology such that its potential, limitations and scope can be more precisely understood and deliberately shaped in a considered manner. With this thesis, in other words, I have sought to interrogate as well as take part in articulating the political possibilities of blockchain technology. Having disassembled and reassembled the 'trust machine' in different ways throughout this thesis, my answer to my overall question then is that in an open, decentralised system many things *potentially* matter when assessing its political implications. What matters more precisely is the site of negotiation, differentiation and dissensus – context and negotiations that are often dismissed (as 'mushy humans', irrelevant speculative behaviour, imperfect communication and so on). A thread throughout the thesis, then, has been to challenge generalised claims made of 'decentralisation' 'trustlessness' and 'consensus' and ground these in the specificity of their enactment through this technology, pointing to their precise enactments and limitations, the dependencies, and relationships with other systems and sensibilities.

In order to answer the question of how to understand the political in relation to blockchain, I have drawn three 'cuts' through the field: first, appropriating Kathryn Yusoff's notion of the *insensible* as a way to point to the limitations and particularity of understandings in the blockchain assemblage of what matters (Yusoff, 2013a), both in algorithms themselves and in

what is intended to be determined through these; second, by tracing and articulating the disruption and *sensibility* of the blockchain assemblage (Rancière, 2006), distinct from political histories and cultures of decentralised network technology, so that I could describe the specific understanding and operationalisation of otherwise broad and universalised concepts; and, finally, by proposing the *dissensible* as a way to describe the ongoing possibility of differing, incompatible sensibilities as the re-emergence of the political and the particular ways in which such dissensibility is negotiated and resolved.

The nature of these 'cuts' has pushed me to draw from a wide and perhaps unusual variety of theoretical sources and debates – from technical papers on cryptography to animism and economics. I have relied heavily on the thinker Karen Barad's work on determinacy and indeterminacy (Barad, 2007) as well as Rancière's work on the political as a disruption to the 'sensible' (Rancière, 2006, 2010), in order to draw a theoretical thread through these disparate sources. Barad's work enabled me to address the deterministic promises in blockchain from a unique perspective, whereby the deterministic qualities of the technologies employed in blockchain can be fully acknowledged while also pointing to the exact boundaries. Rancière, in the meantime, enabled me to relate such an approach immediately to questions of the political, the clashes and negotiations of differing sensibilities, differing understandings of what matters and what should be made to matter. As Barad points out, humans are not the only agencies that determine things (Barad, 2007, p. 338), but, in response to technological determinism in blockchain, neither are the apparatuses that humans build. Such technological determinism is not unique to blockchain. What is unique and important, though, is that blockchain is suggested as a technology intended to be both decentralised and not determined by any specific authority *and* deterministic, determined solely through its code and architecture. This raises important and unusual questions about the exact limits of such different sites of demining things in a decentralised system: through decentralised input, the deterministic apparatus itself, the developers and engineers who designed it, the miners and nodes that run it and so on (the very conundrum explored in Chapter 6 on the *dissensible*). This implies an open question as to the limits of what can or should be determined in the architecture, limits of what matters in the security model, limits of who or what can be involved, and how. Blockchain, because of intentions to eliminate 'authority', replacing this with a 'trust machine' operated through multiple different devices with multiple different versions of the protocol and client, does pose some challenge to defining and analysing a distinct 'thing'. Indeed, the very definition of the 'thing' itself becomes politicised as a question.

With this chapter then, I conclude the thesis by first rearticulating the main insights and contributions of the three 'cuts' I have drawn here, pointing to the implications that these suggest for the literature (sections 7.1 and 7.2 and 7.3). I then discuss this question of limits

that emerged through the thesis and what it implies in terms of relationships to an 'outside' of those limits – diverse economies, different *sensibilities* and so on (section 7.4). I end the chapter, and this thesis, by discussing the limits and scope of my work, suggesting areas for further research (section 7.5).

7.1 Determinacy, trust and autonomy

In this section, I describe and discuss the main findings from my first 'cut' on what matters politically in blockchain, in which I make the *insensible* come to matter in relation to protocols and technical architectures. In this cut, I first described the Bitcoin and Ethereum architectures, discussing these descriptions, purpose and reasoning. By doing so I was able to explain how cryptographic proofs lend a very particular meaning to the concepts of trust, autonomy and decentralisation in blockchain. The ability to cryptographically prove things is operationalised in the Bitcoin architecture to organise a form of computational consensus in a decentralised network, namely the *proof-of-work* consensus algorithm. Describing this algorithm I articulate the precise form of 'consensus' that is assembled, which is on the basis of disinterested, economically-motivated settlement on events intended to be beyond the capacity for any single human to repeatedly determine.[191] Understanding this algorithm enables a discussion of how cryptography is used in the consensus algorithm with the intention and idea of eliminating the need for 'trust'. If events, ownership and access can be cryptographically-determined and secured – and cryptography is mathematically-determined – then there is no longer the need to trust any institution or person's claim. Instead, the truth of events is determined mathematically, no longer requiring external authority or mediation. A main contribution of this chapter is to disassemble this consensus algorithm, emphasising the particularity of this arrangement in order to clarify and make specific otherwise universal claims of having solved the problem of trust and consensus.

This particular method of determining consensus, because it is based on cryptographic proofs rather than trust, is also understood to be an *objective* method for arriving at and enforcing consensus about events. This has led to an understanding of Bitcoin as the invention of 'trustless' consensus, a 'truth machine' implying the elimination of the need for any 'trusted' means for organising consensus and truth of events across any context – from financial to political and legal. I describe how this specific understanding of trust comes from the context of network security engineering for decentralised networks; in order for a decentralised

[191] The 'disinterest' of actors involved in the network is constructed through scale, distance and economic incentives. This construction can be argued as in fact a high level of 'intermediation' in order to construct human engagement as disinterested, and to ensure that there is no direct interest in the results (verified transactions), other than to produce them.

network to be secure, the network as a whole cannot be dependent on (trust) any single aspect of the system, otherwise that particular aspect can become an attack vector to destroy the network. As I argue in Chapter 5, this perspective comes from a politicised pre-Bitcoin history, and I suggest that the context of the financial crisis and the Wikileaks financial embargo lent a broader meaning and appeal to the possibility of trustless systems, referring to untrustworthy government and financial institutions. I argue that through Bitcoin, the remit of conceptions and operationalisation of 'decentralisation' and 'trust', specific and particular to decentralised information networks, are expanded to include all manner of interactions, systems, contexts and institutions. Bitcoin came to represent a general possibility of eliminating the need to trust in any authority to determine and enforce consensus at scale.

Developing this more precise understanding of ideas of trust and decentralisation as understood in Bitcoin enabled me to describe the Ethereum protocol and project, as an explicit project to generalise the Bitcoin architecture and with it, these particular conceptions of trust and decentralisation. The Bitcoin proof-of-work algorithm is seen as a more neutral and objective mediation and enforcement of consensus because it is considered 'trustless', while humans, human judgment are necessarily subjective. The generalisation of this idea of trustlessness, and the particular aim of developing a system without attack vectors, came to imply a system beyond the control of humans in general. By tracing through the concerns in network engineering and the particular contexts and rationale of trust and decentralisation, I was therefore able to explain the reasoning of the use of Ethereum for decentralised applications, Smart Contracts and organisations (DAO) beyond human control, namely that it is a logical extension of the need for systems that cannot be shut down by any authority. This reasoning for systems beyond human control in the meantime also informs the specific understanding in Ethereum of decentralised systems enabling a form of 'autonomy' of the system itself. I discuss the ways that this understanding of autonomy sits in tension with interpretations of decentralisation as enabling a form of autonomy that, on the contrary, implies being *more* in control of systems and conditions that might affect people. In Ethereum, the deterministic qualities of cryptographic proofs and trustlessness, when generalised, become a promise of an autonomous agency of determinacy, an agency that determines transactions, data and relationships in a manner that is beyond control. In other words, the entirely controllable deterministic process of cryptographic hashing gives rise to the possibility of and reasoning for designing systems beyond human control.

I draw on the theoretical work of Karen Barad to rethink these promises and the practices of determinate systems, which allows for acknowledging things that might be determined through the use of cryptographic hashing without therefore having to cede all authority to it. In the Baradian agential realism (Barad, 2007, pp. 132–185), neither scientific apparatuses nor human beings are the only determining 'agencies'. Determinate effects happen through all

manner of what she calls intra-actions at a quantum level, unfolding determinate, material conditions from a field of indeterminate potential in an ongoing manner. This means that cryptography, and importantly also *accounts* of cryptography, can indeed determine things in particular and different ways, but in no way does it therefore necessitate that it be the best, most objective or most appropriate means to determine transactions, truth of events or otherwise. Instead, this must be assessed in relation to a variety of other conditions, contingencies and effects.

I tie these observations and arguments to the question of the pre-condition of the political by drawing in Yusoff's articulation of the *insensible* as that which might not be sensed, but is nevertheless understood to matter (Yusoff, 2013a). Not only are there other agencies that determine matters, these might also never come into direct relation and be sensed as mattering. To put it differently, there is a sense that neither humans nor the apparatuses (or any other probes and prostheses that humans might build) fully sense all that matters (the extinction of lifeforms that we have never known is the question that Yusoff discusses). The importance of this, philosophically, is that there are effects, lives, sensibilities and things that happen that we do not immediately sense and relate to, and that therefore are not sensed as mattering by any attempt at creating a generalised sensibility. It is a consideration that is important for addressing the kind of 'autonomy' that the Ethereum project seeks to achieve, and the idea of algorithmic network agencies that operate beyond the control of humans (and also potentially beyond an immediate relation to human concerns). Yusoff notes, in her work on the Anthropocene, 'These mappings of planetary material infrastructures have an affective economy that place some subjects in and some outside of agency', and points towards the ways that some humans are treated as resources to be extracted (Yusoff, 2013b, 2017). This suggests that 'humans' are not all necessarily on the same side in relation to 'nature'; instead, there are affiliations (and alliances) across human/non-human distinctions, although these might be read as temporary moments of political contestation, before eventually being included in a 'universal' sensibility of what matters encoded in law or treaties or otherwise (for example the amazon, an animal facing extinction etc.) – an understanding of aliveness, affinities and relationships that is nicely captured in Ellen Ullman's autobiographical novel Close to the Machine (Ullman, 2013) describing programmers' affinities to the systems they build over and above a concern for those who use them.

Drawing in Yusoff's work on the *insensible* (2013b), I argue to resituate 'autonomy' as operationalized in Ethereum as a question of affinities that cross distinctions between humans and non-humans rather than suggesting a universal condition. The *insensible* suggests a position in relation to the possibility of autonomous elements in Ethereum (autonomous in the sense of beyond human control) that does not necessitate reasserting claims of complete human oversight and control. In my discussion of blockchain consensus mechanisms and the

kinds of autonomy that is conjured in the design of trustless systems, I aim to contribute to debates on the possibility of an ethics and politics in relation to algorithmic, network systems that defy immediate or complete oversight – notions of opacity, challenges of fully 'knowing' algorithms and their ever-changing emergent behaviours in relation to input challenges ideas of complete knowledge as the basis of responsibility, and as the basis of an ethics and a politics.

Situating Ethereum and blockchain amongst and in relation to other determining agencies, as a question of affinities rather than distinct categories, means that the human versus machine dilemma can be sidestepped, as can awkward questions of aliveness, which I have attempted to address through ideas drawing on animism (see 4.2) and contemporary new materialism debates (2.2.2 and 4.2.2). Instead, affinities are drawn up such that the question of whether a given Smart Contract or DAO is indeed autonomous or not (or whether AI or a coming singularity is 'alive' or not), is not a matter of absolute definition, but of relation to the particular phenomenon. This points to a question of affinities and relationships rather than absolutes, such that some humans might be 'closer to the machine' enabling a certain communication, relation, control or otherwise in a given assemblage, while other aspects operate indeed beyond the control of other humans – a radical relativity which is nevertheless precise and which suggests the presence of the *insensible* in all manner of contexts, that, if taken seriously, demands an extraordinary spaciousness and indeed trust, but that in the meantime avoids the need to replace human or institutional authority with yet another, algorithmic form of authority. In this chapter, then, I described the protocols and architectures as a question of the precondition for the political, seeking its resolution in technological determinacy. I argued to re-open the question of a precondition of the political through, on the one hand acknowledging multiple agencies of determinacy, but also by asserting a certain humility required in the face of the *insensible*, a haunting awareness that what matters might not be immediately sensible.

7.2 Decentralisation and authority

In this section, I describe and discuss the main findings from my second 'cut' on what matters politically in blockchain by articulating a particular blockchain *sensibility*. By understanding what matters, is desirable or undesirable for a blockchain sensibility, a clearer understanding can also be had as to the ways blockchain might be disruptive. By using the term 'sensibility' I have drawn on Rancière's concept that describes a common sense of what is good or bad, desirable or undesirable that cuts across differences and disagreements to comprise a recognisable blockchain assemblage. A key insight gained from this cut is in response to a body of critical literature on blockchain, suggesting that a blockchain sensibility is not primarily

affiliated to right-wing politics, but rather to decentralised network computation. That is not to say that the presence of the right wing and a right-leaning political economy is not significant in the space and ties in to the technology in important ways (Nakamoto, Bridle and Brekke, 2019, p. 62), but instead that there is another sensibility that crosses these differences, and that forms a common sense in the community despite these, which also points to important political possibilities that otherwise would be missed. Gibson-Graham's notion of diverse economies (Gibson-Graham, 2008) allowed me to treat the field firstly as both containing an internal diversity of approaches, such that I would hesitate to associate Bitcoin, Ethereum and blockchain within an exclusively capitalist or right-wing politics. By taking seriously the diversity of people, opinions and ideas that 'blockchain' was attracting I was able to trace through a particular form of disruption and sensibility that is not primarily concerned with capitalism, but rather computation; with decentralised networks as a strategy to circumvent authorities. Notions of diverse economies also allowed me to focus on the many ways that protocols and projects are already dependent on and sit within existing economic dynamics and offer a critique of the ways in which these otherwise tend to be positioned and analysed as wholesale replacement of existing systems. The most evident example of this is the relationship between cryptocurrency exchange rates and protocol security properties – often treated as separate concerns, but that are highly interdependent. Such a perspective foregrounds the dependencies of already existing diversity of fields, which in turn also opens up a focus on articulating these relationships as an important site of political and technical meaning, otherwise often dismissed as not mattering.

In an effort to draw out a blockchain sensibility, then, I traced a pre-Bitcoin history of decentralised network technology and the reasons that decentralisation came to form a specific form of anti-authoritarian strategy: as a means to make it impossible for an authority to shut down or control a network. The main insights from such histories of technical architectures were that the political sensibility of blockchain is grounded in such political histories of network computation more so than political-economic ideologies, and that political economic ideas are instead operationalised in the architectures in order to achieve specific network security properties and behaviours (which were to form the basis of a new interdisciplinary field of cryptoeconomics). More specifically, economic incentives are used in order to achieve security properties in the network: making 'attacks' expensive while rewarding contribution to the network. It is worth noting that the design of 'incentives' lends a certain promise whereby the architecture is understood to be able to determine behaviours at scale in a continuous, immanent manner. The deterministic promises of blockchain protocols are significant in themselves by encouraging such ideas of behavioural engineering – that 'blockchain' can be used to configure societies and used for 'the good', if only coded correctly, incentivising certain behaviours over others. Such temptations of large-scale behavioural engineering also have an attraction that cuts across political ideas and leanings. I would like

to argue that such tendencies represent a form of reconstruction of authority, justified through mathematical determinism. Importantly, tracing through these histories also gave more contextual understanding of key concepts and ideas that form a blockchain sensibility that I explicitly describe in the chapter as commonly desired *principles*, *properties* and *effects* in the assemblage.

Situating Bitcoin, Ethereum and blockchain more generally in such a politicised history of decentralised networks enabled me to articulate two major changes in the development of decentralised technologies in blockchain, namely 'platformisation' and 'tokenisation'. A key insight that I articulate here is the importance of these two developments for debates about platform economics and platform capitalism (Langley and Leyshon, 2016; Scholz, 2016; Pasquale, 2017; Srnicek, 2017). My analysis points towards a nuanced take on the field, suggesting blockchain does not necessarily represent business as usual and yet another instance of platform capitalism. I argue that there is a disruptive proposition not merely based on competition but rather on a different vision for internet and network technologies. With this I therefore aim to re-open some political space in debates on platform economics and blockchain, by drawing in a pre-history of decentralised technologies, such that 'platformisation' can become a project of making privacy-aware protocol design more easily available, and 'tokenisation' as an opening to debate what kinds of economic and governance models might best sustain global network infrastructures.

Ethereum was placed in this longer historical trajectory, and I discussed some of the issues that came about in attempts to platformise 'decentralisation' by making the Bitcoin architecture Turing-complete. I discussed the curious condition of Ethereum as a project to become the general platform, aiming for what can very well be considered a monopoly position as such, being both protocol *and* platform. And yet 'blockchain' is positioned as a 'disintermediating' technology aimed at disrupting monopolies. I sought to explain the ways in which the project, more specifically Ethereum inventor Vitalik Buterin, is able to differentiate the Ethereum platform from other forms of platform intermediation that it seeks to disrupt. This is largely through the idea of 'trustlessness', that the Ethereum protocol and platform is beyond the control of anyone, including the inventor himself. Decentralisation as entailing trustlessness and these conditions as being the main differentiation from other platforms shows a great deal about what matters to a blockchain sensibility. The argument for trustlessness also works to position the Ethereum protocol itself as a form of neutral substrate through which any protocol, currency or system can be designed, deployed and enforced. I argue that this construction of neutrality is based on the very ideas of non-human trustless autonomous systems that I disassemble in Chapter 4. It also places the onus of such claims of disintermediation and disruption heavily on questions of protocol governance as became clear and discussed in Chapter 6.

My analysis of pre-Bitcoin history in the meantime points to other important development pathways, highlighting hopes for blockchain as an infrastructure that might circumvent censorship, sanctions and other forms of geo-political control of network flows. This history is one that is critical of specific authorities and forms of control, and that understands decentralisation as a strategy rather than an aim in and of itself. It is a vision that is reflected in ambitions for Ethereum (and blockchain more broadly) to facilitate a 'Web 3.0' to 'redecentralise' the Internet such that it is no longer dominated by a select few companies, such as Google, Amazon and Facebook. The aim of such a use of blockchain is to disrupt existing business models of the Internet that rely on large-scale data gathering and monopolies both technically and economically. The disruption proposed in blockchain here is that by decentralising data storage and verification, data monopolies would be made technically impossible, and by incorporating economics into the protocol design, some level of economic independence might be achieved such that network infrastructures would no longer be dependent on extractive business models. There are nevertheless significant challenges to such a vision for blockchain, in terms of protocol governance as well as in the complexity of incorporating economic dynamics in the protocol in what I discuss as 'tokenisation' of decentralised technologies.

I discussed tokenisation by focusing on two points; first, the complexity that protocols are opened up to when economic dynamics are incorporated in their function, issues that the field of 'cryptoeconomics' grapples with; and second, the shift in political economic assumptions in network culture that tokenisation brings about. In generalising the Bitcoin architecture, Ethereum platformised the capacity to create decentralised value tokens introduced in Bitcoin: new blockchain projects that did not have a sufficient network to run a decentralised currency could 'bootstrap' the Ethereum network to launch new tokens, using a simple Smart Contract. Furthermore, the Ethereum architecture also generalised the use and function of tokens, making these the 'fuel' of a decentralised computational network, running Smart Contracts and means for governing organisations (DAOs). The intention of internalising economic dynamics, as mentioned above, is to achieve network security properties by encouraging computational contribution to the network as well as the possibility of a certain economic autonomy for the protocols by creating an internal economy. However, a key insight and argument I make is that that by incorporating economic dynamics into the security model of the protocol, the protocol itself is opened up to all manner of economic dynamics and complexities which challenges any deterministic claims made of the security properties.

A second observation of the consequences of tokenisation was the ways this significant new element in protocol design affects the political economic assumptions of network culture more generally, and the imagined use-cases of blockchain. Pre-Bitcoin network culture was largely defined by the idea of networks as facilitating flows, and as representing a form of abundance

through the near-zero cost of digital copies. This was a foundation for a certain critique of property, in particular intellectual property (cf. Terranova, 2004; Coleman, 2009; Söderberg and Daoud, 2012; Rifkin, 2014; Arvanitakis and Fredriksson, 2016). With the invention of decentralised digital tokens in Bitcoin and the generalisation of their use in Ethereum, the tools for designing digital scarcity were also decentralised, which, I argue, orientates ideas and use-cases towards ever more fine-grained determination of property and property rights and their enforcement – a subtle but significant shift in the political economic assumptions in decentralised network culture, and one that directs a blockchain sensibility towards particular kinds of use-cases and projects.

7.3 Dissensus and indeterminacy

In this section, I describe and discuss the main findings from my third and final 'cut' on what matters politically in blockchain, proposing the concept of the *dissensible* to describe the ongoing possibility of different sensibilities, their potential incompatibility, and the question of their resolution. When both Bitcoin and Ethereum faced crises around development pathways, this raised the issue of who is to determine decentralised systems in the first place. This turned the attention of the blockchain industry more generally towards protocol governance and the question of, 'Who is responsible for making the decision on how to make decisions?' (Kreutler, 2018). If Bitcoin, Ethereum and blockchain were indeed a form of disintermediation, whereby decentralised, trustless protocols would replace the need for authorities, then the protocols themselves would also need to be determined in a decentralised trustless manner. I have described these crises and debates as a re-emergence of *the political* introducing the notion of the dissensible to point towards compatible sensibilities and their negotiation. I analyse them as a renegotiation of the purpose, aims and implications of blockchain consensus in response to the re-emergence of 'dissensus' – that through these crises, the communities in and around Bitcoin and Ethereum and the blockchain industry grappled with ways to accommodate for *dissensibilities*, in a manner that nevertheless would be consistent with a blockchain sensibility, rearticulating decentralisation, trust and consensus in the process. I have done this by tracing through the conflicts, describing the ways in which open, collaborative coding processes of git and GitHub became foregrounded as governance mechanisms, and how the idea of 'forking' code, blockchains and projects become a means for resolving dissensus, what I describe as a 'dissensus mechanism' in the field.

I introduced the notion of the dissensible as a concept to describe differing sensibilities of what matters. I describe the Bitcoin scaling conflict therefore as entailing differing understandings of what matters in terms of increasing the capacity of the network, but also as an expansion of what matters in terms of Blockchain protocol design more generally – from

the protocol itself to include hidden and not-so-hidden power dynamics, mining hardware and centralisation of mining, company affiliations, currency holdings, and stakes in different outcomes, different priorities in terms of development pathways, and so on. One insight gained from this description was the way in which Bitcoin protocol governance was foregrounded as mattering for claims of decentralisation. Descriptions began to include economics in order to argue for 'decentralisation' at the level of protocol governance, arguing that not only developers and miners but also holders of bitcoin have a say in the direction of protocol development, as the value of the system is dependent on their use of the system. I suggest that this is a strenuous claim that nevertheless points to some of the ways that 'decentralisation' remains a main concern and reason for the system, all of which came to matter in questions of who gets to determine 'Bitcoin' in the first place. It is a question of the limits of the design space in terms of protocol design concerned with and dependent on 'decentralisation'. A key insight here is that the claims and desired properties of 'decentralisation' on a protocol level, namely that it be beyond the control of authorities, is nevertheless severely affected by centralisation elsewhere, for example in terms of mining hardware or currency holdings. This issue is addressed in several ways, one of which is to seek further decentralisation in these other areas, which begs the question of limits of what should be considered to matter, and be part of the 'design space' of the protocol, or what should be taken care of by other means. Indeed, an issue of limitations to how much blockchain can or should determining things (transactions, or consensus more generally) that I discuss in 7.4 below.

The Bitcoin scaling conflict highlighted different understandings of the aim of Bitcoin that can be gleaned in discussions from even the early days; namely whether the purpose of a decentralised payment system is as a strategy to circumvent authorities and 'formidable adversaries', or whether the priority should be to compete with existing payment systems in terms of speed, seeking mainstream adoption and recognition from regulators. The two positions are not entirely mutually exclusive, but emphasise different approaches to authorities and regulation in particular, and in terms of priorities in the technical development that became increasingly incompatible.[192] I describe how attempts at conjuring the original author(ity) played in to the conflict when Australian businessman Craig Wright claimed to be Satoshi Nakamoto, the inventor of Bitcoin, aligning with the development pathway promoted by Bitcoin Foundation members Jon Matonis and Gavin Andresen. This attempt was thwarted as Craig Wright failed to produce the only kind of evidence that might have been acceptable to a community formed around the possibility to eliminate authority through trustless

[192] – a difference in vision for Bitcoin as a project, which could be summarised as legal recognition versus a 'Darknet'. In this thesis I have avoided discussions of Bitcoin and the 'Darknet', however, because it opens up a series of new debates around the use of bitcoin for illegal activities, legislation and so on which, though related, are beyond the immediate scope of this thesis.

architectures and decentralisation, namely cryptographic proof. The incident brought to light the strongly anti-authoritarian tendencies in Bitcoin and blockchain sensibility.

In my discussion of the Bitcoin scaling conflict I highlight how what might be perceived as purely technical decisions embody particular priorities and development pathways that can quickly become hugely politicised – and, conversely, how differences and disagreements are often construed as information security questions in the community. This serves to depoliticise decisions that might entail broader questions about who is best served by a given decision, instead framing the debates in the realm of security concerns that are considered neutral and beyond special interests. The question of whether to increase capacity by changing the protocol and increasing blocksizes or whether to increase capacity by enabling other layers, 'lightning network' and 'sidechains' and so on also became a question of different priorities in terms of a project of decentralisation – whether to compete with existing systems along existing terms such as speed and convenience, generally associated with an increase in blocksize, or whether to prioritise decentralisation at a protocol level representing an alternative to existing payment systems along questions of governance and decentralisation instead. These different positions were muddled by different affiliations with companies and interests in the outcomes, whereby, for example, the Bitcoin developers advocating to keep the current limit on blocksize on the basis of protocol level decentralisation tended to be working with the company Blockstream who, in the meantime, were developing alternative solutions for scaling and capacity. I then describe the eventual resolution through the Bitcoin Cash hard fork leading to two incompatible versions of Bitcoin.

In my discussion of the Ethereum DAO hack I highlighted how the crisis, and fork that followed, challenged one of the main preconditions and promises of a disinterested, algorithmic mode of determinacy, namely immutability. Decentralisation, code and cryptography were supposed to ensure that the blockchain could not be controlled and would execute exactly as coded, which required that the code and the blockchain be immutable. The DAO hack and subsequent hard fork by the Ethereum Foundation demonstrated that what is written in immediately executing code might not play out as intended, that intentions indeed are important and that Smart Contract code, as well as the blockchain itself, can be corrected and controlled by human decisions; the question is simply by whom and under what conditions. I describe how the decision of the Ethereum Foundation to hard fork therefore caused major reconsideration of the purposes and intent of decentralised systems. Where the Ethereum project had distinguished itself as a platform beyond the control of anyone, including the Ethereum Foundation and Vitalik Buterin, the inventor himself, the hard fork for some represented a major disappointment of that promise. I discussed the role of 'forking' in resolving this issue in a way that would be consistent with ideas of decentralisation, namely as a *dissensus mechanism*. Those who were unhappy with the Ethereum Foundation fork

retained the previous version of the Ethereum blockchain as 'Ethereum Classic', such that there would be two versions of Ethereum entailing two visions for what matters in terms of the Ethereum blockchain platform, and indeed how dissensus should be resolved. For some, the solution was to expand the remit of an algorithmic mode of consensus, while for others the hack became a reason to address more carefully the relationship between blockchain systems and complex social processes, a 'social contract'. A key insight of tracing through debates in and around The DAO hack, therefore, is that its resolution emphasised different understandings of decentralisation, trustlessness and control, one aiming to extend the form of determinacy suggested in the consensus algorithms to protocol governance itself, in what is called on-chain governance, and one that includes the possibility of 'the social' to determine aspects of how protocols should develop whereby forking operates as a form of vote. This latter perspective retains the claim of a system beyond control of authorities, now no longer conveying that authority to an algorithmic process, but instead understanding the system architecture to facilitate decentralised social determination – on the basis that protocol changes by developers rely on adoption by miners, full nodes and those using the systems.

I draw on some of Mouffe's analyses of liberal institutions whereby the understanding of these as 'universal' mediums through which politics might play out in the meantime depoliticises contestation of these, reconfiguring the political into a moral question (Mouffe, 2005, pp. 69–89). Contestation that happens outside of what are understood as the legitimate forms established by liberal institutions are labelled as bad and immoral on the basis of being undemocratic. I compare this reconfiguration of the political to blockchain systems. Blockchain, as a different form of proposition for a neutral substrate on top of or through which difference might be negotiated brings with it its own 'legitimate' forms of contestation. No longer a moral question, in blockchain, the legitimate form that dissensus can take is as a network security question – whether a given action is a bug or a feature, an attack or exploit. Addressing all behavioural aspects as network security concerns allows the system to continue to be understood as neutral and universal, rather than entailing and enforcing certain understandings of what should or should not be allowed. Both the scaling conflict and The DAO hack in the meantime pointed to the limits of the idea of neutral, universal systems. The ability to fork the project reference client and blockchain largely represented the resolution to such issues in ways that would remain consistent with ideas of decentralisation and openness.

The importance of protocol governance is not merely a practical issue of who gets to decide and on what basis, but rather addresses the very core of the argument of a decentralised, trustless technology. It is what differentiates blockchain from other forms of platform intermediation and is the basis of its claim as 'disintermediating'. Addressing governance adequately, not as a final algorithmic resolution to authority in the abstract, but in concrete

terms for specific situations – for example, a Web 3.0 – might very well position the technology in interesting and powerful ways in relation to existing corporate or institutional 'authorities'. This raises the question of what kind of determinacy is the most appropriate for different kinds of spaces and concerns. The Bitcoin scaling conflict and DAO exploit were two events that raised the question of limits to the specific method of determining things represented in consensus algorithms and blockchain systems. I would like to argue that this does not necessitate nor validate the assumption of 'human' control, but instead that there is still much to understand about the limitations and possibilities of algorithmic mediation in and among other methods for determining things, processes and relationships.

7.4 Limits, edges and relationships

The question of limits, edges and relationships kept coming up as an unresolved question in the three 'cuts' that I have articulated in this thesis: firstly, the limits to what can and should be determined through an algorithmic sensibility, the edges of such a determinacy and its relationship to other determining agencies and systems and indeed its non-relation to the *insensible*; secondly, the importance of the already existing, yet mostly unacknowledged relationships with existing diversity of economic, monetary, legal and political systems, and therefore the edges and limitations of what different protocol designs can or should involve in those fields; and thirdly, the negotiation over the limits of what should or should not matter in an open, decentralised protocol and how such negotiations are governed and resolved. One of the main, and arguably cross-disciplinary, contributions of this thesis is to raise this question of limits and edges as an important question for decentralised open blockchain systems to address and articulate – pointing towards the need also to address and shape relationships to pre-existing systems and contexts more explicitly, whether enforcing these, disrupting them, being dependent upon them or otherwise. I therefore briefly address this underlying thread more explicitly, before concluding the overall thesis by suggesting further areas of research.

The issue of limits, edges and relationships first comes up in the analysis and discussion of limits to 'trustlessness'. Analysing the protocols of Bitcoin and Ethereum highlighted how claims made of these can indeed be read as true in some instances and for some purposes but not for others. Here, I was faced with the question of the exact limits to such claims that I discussed in 4.1.2 specifically in terms of trustlessness and 4.1.3 in terms of decentralisation. I analysed where they came to matter in terms of correction and enforcement; which precise aspects of a specific protocol design should be 'trustless' and 'decentralised' in order to achieve the desired properties and effects, instead of assuming, as much of the industry seemed want to, that general statements could be made about these. There was a tendency

to describe the condition of a system that simply was not true in terms of interactions with it. I found some explanation to this widespread tendency by tracing through politicised histories of decentralised networks. I drew on the example of file-sharing networks in particular, and found that there was a logic at play here whereby the file-sharing networks themselves, by being decentralised, were indeed used as a strategy to make these resilient to authorities' attempts at shutting them down, but that this did not translate into such resilience for individuals who regardless would be arrested and prosecuted. What I read in this was a seed of what was to become a widespread tendency in blockchain to affiliate with a given system and the condition of a system over and above the individual engagement and uses of it; the grounds for what was expressed on the Bitcoin developers' mailing list as the difference between the 'perfect system' and 'mushy humans'. What became clear was that what might be considered true for the given system, for example 'trustlessness', is not necessarily true for those using it. I raise the issue of limits, edges and relationships in terms of the protocols, then, to argue for the need to make specific the claims and aims of open decentralised systems – for who exactly they are trustless and decentralised and what trustlessness and decentralisation is supposed to achieve more precisely. That is not to say that they need to be trustless and decentralised for each and every context, but rather to argue for some consideration of what might be the appropriate uses of 'trustlessness' and 'decentralisation' as technical and political strategies to achieve certain effects, rather than as aims in and of themselves.

The question of limits, edges and relationships came up secondly when articulating and analysing the form of determinacy sought through the employment of cryptographic hashing and decentralisation. The configuration of these elements was based on an understanding of an objective system as a system beyond control. This form of 'objectivity', created by assembling such a 'truth machine', entailed that anything *not* determined through such trustless mechanisms might be dubious, and in the meantime entailed a demand for expansion of such a form of determinacy. This was evident in two examples; firstly, the question of Smart Contracts and the necessity of expanding their remit to physical objects such as locks and so on, in order for the immediately executing laws of code to be effective; and secondly, in responses to The DAO fork in Ethereum that demanded that the governance of protocols also be determined in and through such 'truth machine' mechanisms. Both of these examples pointed to the question of the limits to what can and should be determined by 'blockchain' and to the unresolved issue of the relationship between such mechanisms and other forms of determinacy, or indeed, the indeterminate and insensible. In part, this could be articulated as an issue of infinite regression in a pursuit of a resolution to the issue of the dissensible: a consensus algorithm to determine consensus, which would require a consensus algorithm to determine consensus about the consensus algorithm, and so on – namely the problem that was raised and being grappled with in both the Bitcoin scaling

conflict and the Ethereum DAO exploit. But the question of infinite regression is a conceptual and hypothetical one. More urgent, real and important is the problem that by assuming the resolution of authority and the political in a 'truth machine', one delegitimises any other determining agency as well as the *insensible*, in essence recreating an algorithmic authority that determines things on the basis of, in the case of proof-of-work, competitive, and probabilistically decentralised hashing cycles. The question of limits, edges and relationships here is one of addressing more deliberately what might be appropriate uses of such a method for determining things and relationships and with what aims. By making such methods specific and limited to specific uses, it thereby also opens the possibility to address more deliberately how such methods in turn relate to other forms of determining things (whether existing legal systems, economic or monetary conditions or otherwise). In response to this question, I look to rescue some of the particular disruptive potentials of a blockchain sensibility – in particular, to foreground a main disruptive aim, namely Web 3.0 and the aim of making mass surveillance-based internet business models technically and economically unfeasible. Such an aim requires a specific application of blockchain, less as a solution to authority and the political in general, and more as a proposition for different kind of internet infrastructure and governance mechanisms.

The need to incorporate and determine more and more things through a deterministic protocol in the meantime opens up such a protocol to all manner of dynamics raising the question of limits, edges and relationships in terms of what matters in the security models in the design of open decentralised network protocols. The remit of blockchain protocols are often discussed in a hermetic manner, a given protocol assessed on its own terms, and relationships to other systems largely limited to an articulation of attack vectors in dystopian or utopian speculation that assumes blockchain to completely replace existing systems. In the meantime, blockchain projects and protocols are built within the context of, in response to, and are dependent on existing socio-political and economic contexts, systems and dynamics. The relationships to such other spaces and dynamics matter significantly, although they tend to be excluded from discussion and analysis exactly because they do not correspond with claims of trustlessness. I discuss these edges and relationships more specifically in relation to, firstly, claims of decentralisation and disintermediation, and secondly in relation to exchange rates and the network security assumptions of the profitability of mining. During the Bitcoin scaling conflict, new things came to matter in terms of protocol design, namely their governance and the extent to which their governance could be argued to be decentralised, and therefore trustless. In response, there were efforts to measure levels of decentralisation in terms of protocol governance, including contributions to core clients, mining, mining hardware and so on – expanding the realm of what matters in terms of the security model itself. This raises the question of the edges of what matters, in terms of decentralisation and the security model of, in this case, proof-of-work, as the protocol is dependent on its maintenance, miners

incentives, electricity costs, mining hardware, chip production and so on. All of which could *potentially* matter in terms of network security, if these were not determined and taken care of through other means and reasons. For example, the reason for why the rather centralised miners do not collude to cheat the Bitcoin network might have as much to do with questions of reputation, legitimacy and so on than the immediate value of their bitcoin holdings. Such complexities are the subject of the field of cryptoeconomics that looks to model and operationalise such assessments and behaviours through game theory and psychology. Here, also, is an issue with limits and the mostly unacknowledged forms of relationships to the fields and dynamics that are *not* incorporated into the protocol. This came up largely in curious attempts at dismissing the importance of exchange rates for blockchain protocols. The incorporation of tokens into decentralised protocols is argued to ensure certain security properties (making it expensive to attack and reward contributions). This was informed by hopes and ambitions for a certain economic autonomy to be gained by incorporating tokens. Creating a token is not the same as creating an economy, however. Instead, it draws in new forms of dependencies on monetary and economic dynamics beyond the protocol.

Overall, then, what was highlighted was the importance of articulating such limits, edges and in particular the relationships that are formed, whether deliberately or inadvertently, in order for blockchain to regain a situated meaning and purpose. There is much to be disentangled and resolved her in terms of claims of 'disintermediation', and much that could be explored more deliberately in terms of relations to existing systems (economic, legal, geo-political and so on) and the effects on one another. In terms of a blockchain *sensibility*, the projects where relationships and purposes are indeed articulated the most clearly are those that relate to privacy, censorship and network control – the explicit and deliberate efforts to develop networks of communication and value transfer that cannot be shut down by specific state and financial authorities. Note that such projects do not have to imply an assumption of having resolved *all* issues of authority through 'trustlessness and decentralisation' in order to be achieved, but they do need to consider questions of governance of such means of authority-resistant communication and value transfer in order to survive in the longer term. Instead of resolving the problem of consensus without authority in absolute abstract terms, then, it is enough to solve it for specific purposes, and in the process articulate a new form of network space and governance of such space that might indeed disrupt existing political and financial authorities.

7.5 Scope and further research

With this thesis I have sought to address foundational questions of *the political* in relation to a technology that seeks to 'solve' it in ways that would remain consistent with rigour and

practices in computer sciences, political and social sciences alike. The scope of this thesis has therefore been limited to this effort of shifting and clarifying some of the terms of the debates about blockchain technologies. This has meant that, while I have gone into detail in my analysis of certain key concepts, their provenance and operationalisation in technical efforts and events, there are questions that I have dealt with on very abstract basis, only hinting towards empirical material, the most glaring of which is a 'user' side to the protocols and applications. Just to mention a couple of examples: to understand the attraction of 'decentralisation' more broadly beyond an immediate Cypherpunk and blockchain cultures; what specifically attracts application developers to develop on decentralised platforms rather than existing app stores (and what this says about 'disruption'); the practical usability of decentralised payment infrastructures to actually circumvent sanctions or banking blockades. I conclude this chapter suggesting a few more possible areas of research and theoretical work from this thesis.

In my discussion of blockchain protocols I argue that the cryptography, decentralisation and economic incentives that form a blockchain 'truth machine' cannot be considered 'neutral' and 'objective' but rather enforce a very particular form of consensus, which matters. I argue therefore that the protocol itself is a form of intermediation. This implies that 'mediation' cannot not simply be addressed as an unnecessary barrier, or cost, that needs to be 'disintermediated', but in fact matters qualitatively for how things come to matter and are resolved. This includes the protocol itself as a form of intermediation, that it changes things – the quality and type of relationships – rather than simply facilitating these. There are, therefore, significant philosophical, social, technical and political questions that would benefit from further research in terms of the qualitative effects different of forms of intermediation, in particular by addressing these as *sensibilities* rather than systems. This could be, for example, in terms of the question of 'trust' and 'trustlessness', whether and when 'trustless' systems indeed might *enable* trust, by cryptographically guaranteeing a certain neutral terrain given a specific context, or when and under what conditions it might do the opposite, producing trustlessness by militarizing relationships. Another might be on the question of autonomy and autonomous networks and how network technologies relate to experiences of control, being in control or being at risk.

Another area of further research is opened by my discussion of blockchain sensibilities. I suggest that what holds a blockchain assemblage together is not an affiliation with particular extreme Right or capitalist economic ideas, but rather a politicised anti-authoritarian history of decentralised network infrastructures that tie in to and are attractive to different economic ideas. More specifically, I suggest that this opens up an appreciation of the 'platformisation' and 'tokenisation' of decentralised infrastructures as a possible disruption to existing internet platform economies. This has implications for, and suggests important further research in the

areas of infrastructure governance, digital finance, platform economics and platform capitalism, as an urgent task of shaping the stakes and possibilities in the fields. If indeed technical architectures that make centralised control of data impossible are 'platformised', disrupting the possibility of data monopolies, such an agenda would require significant theoretical and empirical work, not only from technical sciences, but also from social sciences that might build towards such agendas and assess whether and how such a possibility might be enacted. Furthermore, if indeed 'tokenisation' might enable if not 'a system that pays for itself' then at least a different set of economic dynamics through which to run global network infrastructures, such an agenda demands significant theoretical and empirical work to shape how such new digital economies might turn out. This could range from exploring the business models appearing in the space, and how they might look different to those enabled through 'surveillance-based' platforms, to the remit for a commons-based approach to the forms of relationships assumed, enabled or ignored in cryptoeconomics, to give just one example. I argue that there is significant space within a blockchain sensibility for such agendas to be addressed from multiple different economic, political and indeed ethical perspectives.

One of the main ways that 'blockchain' is considered different from major internet platforms such as Facebook, Google and Amazon is that it is 'decentralised' and 'trustless'. While much can be and has been said about the limits of these claims (in this thesis as well as in a growing body of critical literature), in my discussion of the two major blockchain networks Bitcoin and Ethereum these proclaimed differences do come to matter, especially in questions of protocol governance. On a protocol level in blockchain there remains a certain sensibility about how code and data is handled that indeed can present a technical, economic and political disruption. But this also means that the governance of such protocols becomes a major issue in the writing of the code and would need to be addressed in ways that achieve the desired results of decentralisation and trustlessness – which, at present, are most strongly articulated for questions of privacy and censorship resilience but otherwise remain vaguely defined, assumed to be important in and of themselves. Blockchain is one of the few technical fields where governance questions are taken very seriously at a structural level and is part of engineering decisions. While governance is a big topic in blockchain debates, there is a significant lack of in-depth research, empirically and theoretically on the issue, which would benefit, in particular, from further research from social sciences and humanities. As an example, the question of accountability in particular is lacking, probably due to an assumption that if authority has been dealt with through decentralisation, questions of accountability are no longer pressing. There is scope for accountability to be addressed, both within a blockchain sensibility around the notion of transparency and also for more fundamental and philosophical ideas and research on the question in relation to decentralised infrastructural intermediation.

Finally, there is significant further theoretical work that could be pursued for a new materialist-informed political theory. In this thesis, I have drawn heavily on work by Karen Barad (Barad, 2007) and Jacques Rancière (Rancière, 2006, 2010) in order to articulate an approach to the political in relation to open, decentralised systems that also claim determinate properties. I have in the process suggested (and assumed significant compatibility between) Rancière's notion of sensibility (Rancière, 2010, pp. 27–44) and Barad's sensing and measuring apparatuses (Barad, 2007, pp. 132–185) – such that Rancière's conceptualisation of the political as a redistribution of the sensible can be understood as part of an onto-epistemological determining process, although of different kinds of scales and complexity than in Barad's examples of specific scientific experiments. Sensibility as well as the political thereby become possible and happen through sensibilities, a sensing device, consensus mechanism and human perception alike, although in significantly different qualitative ways, with differing material outcomes. These qualitative differences become the main site of question, then, rather than *a priori* assuming a site for the political proper or scientific proper; objectivity and subjectivity. The *insensible* and *dissensible* can then be explored as challenges to any singular, linear or complete understanding of what matters and how the sensible becomes material. There is much to research further in such an articulation of these two theorists, in particular how materiality and temporality affect such developments, how different modes of determination in turn affect one another and the ways in which framing networks in terms of sensibilities relate to the more common approach of addressing these as systems and system diagrams. The insensible and the dissensible also suggest that rather than disruption, after which the political moment entails a 'redistribution of the sensible' and 'inclusion' of 'externalities' into such a sensibility, 'forking' and the resulting questions of compatibility or incompatibility might suggest a new and different basis from which to explore and articulate *the political*.

Bibliography

Alcazan *et al.* (2012) *Tecnopolitíca, internet y r-evoluciones sobre la centralidad de redes digitales en el #15M*. Barcelona: Icaria.

Amoore, L. (2006) 'Biometric borders: Governing mobilities in the war on terror', *Political Geography*, 25(3), pp. 336–351.

Amoore, L. (2007) 'Vigilant Visualities: The Watchful Politics of the War on Terror', *Security Dialogue*, 38(2), pp. 215–232.

Amoore, L. (2013) *The Politics of Possibility, risk and security beyond probability*. Durham and London: Duke University Press.

Amoore, L. (2014) 'Security and the incalculable', *Security Dialogue*, 45, pp. 423–439.

Amoore, L. (2015) *Cloud Geographies: Computing, Calculation, Sovereignty*. Exeter: RGS.

Amoore, L. (2016) 'Cloud geographies : computing, data, sovereignty', *Progress in Human Geography*.

Amoore, L. and Raley, R. (2017) 'Securing with algorithms: Knowledge, decision, sovereignty', *Security Dialogue*, 48(1), pp. 3–10.

Andresen, G. (2015) *BIP: 101, Increase maximum block size*, *GitHub* [online]. Available at: https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki (Accessed: 20 January 2015).

Appadurai, A. (2015) 'Mediants, Materiality, Normativity', *Public Culture*, 27(2 76), pp. 221–237.

Arvanitakis, J. and Fredriksson, M. (2016) 'Commons, piracy, and the crisis of property', *TripleC*, 14(1), pp. 132–144.

Assange, J. *et al.* (2012) *Cypherpunks, Freedom and the future of the internet*. London and New York: OR Books.

Azouvi, S., Maller, M. and Meiklejohn, S. (2018) Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance.

Back, A. (2002) 'Hashcash - A Denial of Service Counter-Measure' [online] Available at: http://www.hashcash.org/papers/hashcash.pdf (Accessed: 20 January 2015).

Back, A. *et al.* (2014) 'Enabling Blockchain Innovations with Pegged Sidechains' [online]. Available at: https://blockstream.com/sidechains.pdf (Accessed 4 October 2016).

Ball, J. (2011) 'The bankers' blockade of WikiLeaks must end', *The Guardian*, 24 October [online]. Available at: https://www.theguardian.com/commentisfree/2011/oct/24/bankers-wikileaks-free-speech. (Accessed: 6 December 2015).

Bambrough, B. (2018) 'Bitcoin Believers Speak Out In Venezuela As Maduro Makes Historical Devaluation', *Forbes*, August [online]. Available at:

https://www.forbes.com/sites/billybambrough/2018/08/20/bitcoin-believers-speak-out-in-venezuela-as-maduro-makes-historical-devaluation/#6c86bc1245ae. (Accessed: 16 September 2018)

Bano, S. *et al.* (2017) 'Consensus in the Age of Blockchains' [online]. Available at: http://arxiv.org/abs/1711.03936.

Barad, K. (2007) *Meeting the Universe Halfway*. Durham and London: Duke University Press.

Bauwens, M. (2014) *Spanish Robin Hood Enric Duran on Capitalism and 'Integral Revolution'*, *Shareable* [online]. Available at: http://www.shareable.net/blog/spanish-robin-hood-enric-duran-on-capitalism-and-integral-revolution. (Accessed: 4 April 2015)

Ben-sasson, E. *et al.* (2014) 'Zerocash: Decentralized Anonymous Payments from Bitcoin' [online]. Available at: http://zerocash-project.org/media/pdf/zerocash-oakland2014.pdf (Accessed: 19 October 2015)

Bennett, J. (2010) *Vibrant Matter: A Political Ecology of Things*. Durham and London: Duke University Press.

Bird-David, N. (1999) '"Animism" Revisited: Personhood, Environment, and Relational Epistemology', *Current Anthropology*, 40(February), pp. 67–91.

BitFury Group (2015) 'Proof of Stake versus Proof of Work' [online]. Available at: http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf. (Accessed: 23 January 2016).

Bjerg, O. (2016) 'How is Bitcoin Money?', *Theory, Culture & Society*, 33(1), pp. 53–72.

Blockchain (2018) *The State of Stablecoins*, *Blockchain* [online]. Available at: https://www.blockchain.com/research. (Accessed: 2 December 2018)

Blum, M., Feldman, P. and Micali, S. (1988) 'Non-interactive zero-knowledge and its applications', in *Proceedings of the twentieth annual ACM symposium on Theory of computing - STOC '88*. New York, New York, USA: ACM Press, pp. 103–112.

Bollier, D. (2014) *Faircoin as the First Global Commons Currency?* [online]. Available at: http://bollier.org/blog/faircoin-first-global-commons-currency. (Accessed: 6 May 2015)

Bonneau, J. *et al.* (2015) 'SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies', in *2015 IEEE Symposium on Security and Privacy*. IEEE, pp. 104–121.

Bradbury, D. (2014) 'Unveiling the dark web', *Network Security*. Elsevier Ltd, 2014(4), pp. 14–17.

Braidotti, R. (2013) *The Posthuman*. Cambridge and Malden: Polity Press.

Bratton, B. (2016) *The Stack: On software and sovereignty*. Cambridge (MA) and London: MIT Press.

Bria, F. and Roio, D. (2014) *D3.1 - Theoretical Framework on future knowledge-based economy* [online]. Available at: https://dcentproject.eu/wp-content/uploads/2014/03/D3.1-final_new.pdf. (Accessed: 17 January 2015).

Burrell, J. (2015) ‘How the Machine “Thinks:” Understanding Opacity in Machine Learning Algorithms’, *Ssrn*, (June), pp. 1–12.

Buterin, V. (2014) *Slasher: A Punitive Proof-of-Stake Algorithm*, Medium [online]. Available at: https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/ (Accessed: 2 October 2018).

Buterin, V. (2015) *Visions, Part 1: The Value of Blockchain Technology*, Ethereum Blog [online]. Available at: https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/ (Accessed: 29 July 2015).

Buterin, V. (2016a) *A Proof of Stake Design Philosophy*, Medium [online]. Available at: https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51 (Accessed: 2 October 2018).

Buterin, V. (2016b) *CRITICAL UPDATE Re: DAO Vulnerability*, Ethereum Blog [online]. Available at: https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/ (Accessed: 11 July 2016).

Buterin, V. (2017) *Notes on Blockchain Governance*, Personal blog [online]. Available at: https://vitalik.ca/general/2017/12/17/voting.html (Accessed: 1 October 2018).

Buterin, V. (2018) *Governance, Part 2: Plutocracy Is Still Bad*, Personal blog [online]. Available at: https://vitalik.ca/general/2018/03/28/plutocracy.html (Accessed: 1 October 2018).

Buterin, V. and Griffith, V. (2017) *Casper the Friendly Finality Gadget* [online]. Available at: https://arxiv.org/abs/1710.09437 (Accessed: 1 November 2017).

Buterin, V., Hitzig, Z. and Weyl, G. E. (2018) ‘Liberal Radicalism : Formal Rules for a Society Neutral among Communities *’[online]. Available from: https://arxiv.org/abs/1809.06421 (Accessed: 18 September 2018).

Caffyn, G. (2015) ‘What is the Bitcoin Block Size Debate and Why Does it Matter?’, *Coindesk*, August [online]. Available at: http://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/ (Accessed: 25 August 2015).

Callon, M., Law, J. and Rip, A. (eds) (1986) *Mapping the dynamics of science and technology: sociology of science in the real world*. Basingstoke: Macmillan.

Champagne, P. (ed.) (2014) *The Book of Satoshi*. e53 Publishing LLC.

Chandler, S. (2018) ‘How Venezuela Came to Be One of the Biggest Markets for Crypto in the World’, *Cointelegraph*, September [online]. Available at: https://cointelegraph.com/news/how-venezuela-came-to-be-one-of-the-biggest-markets-for-crypto-in-the-world (Accessed: 7 January 2019).

Chaum, D. (1998) *Blind Signatures for Untraceable Payments*. Santa Barbara: Springer-Verlag.

Cheang, S. L., Rivoire, A. and (eds.) (2015) ‘We grow money we eat money we shit money’. Magazine des Cultures Digitales [online]. Available at: www.digitalmcd.com (Accessed: 6 February 2016).

Choi, J. (2017) ‘Cryptoeconomics’ [online]. Available at: https://www.unitimes.io/file/pdf/04-Cryptoeconomics-in-Casper.pdf (Accessed: 10 June 2018).

Christian, M. (2014) ‘Bitcoin - Asset or Currency? Revealing Users’ Hidden Intentions’, *Twenty Second European Conference on Information Systems*, pp. 1–14.

Coleman, G. (2009) ‘Code is speech: Legal tinkering, expertise, and protest among free and open source software developers’, *Cultural Anthropology*, 24(3), pp. 420–454.

Coleman, G. (2014) *hacker-hoaxer-whistleblower-spy, The many faces of anonymous*. London: Verso.

Community-based Participatory Research: Ethical Challenges (2011). Durham.

Constable, S. (2017) ‘Why Bitcoin Still Isn’t Money’, *Forbes*, 11 December [online]. Available at: ‘Why Bitcoin Still Isn’t Money’, *Forbes*, 11 December (Accessed: 11 January 2018).

Crypterium (2018) *Venezuela’s hopes for crypto: can it save the collapsing economy*, Medium [online]. Available at: https://hackernoon.com/world-crypto-map-venezuelas-hopes-for-crypto-88fcecd04812 (Accessed: 19 December 2018).

Daniel, J. W. (2008) ‘Net Neutrality... Seriously this Time’, *IEEE Internet Computing*, 12(3), pp. 86–89.

Daston, L. and Galison, P. (1992) ‘The Image of Objectivity’, *Representations*, 0(40), pp. 81–128.

DeLanda, M. (2004) ‘Material Complexity’, in Leach, N., Turnbull, D., and Williams, C. (eds) *Digital tectonics*. Chichester: Wiley-Academy, pp. 14–21.

Didil (2017) *Enterprise Ethereum: Private Transactions with Quorum*, Medium [online]. Available at: https://medium.com/@didil/enterprise-ethereum-private-transactions-with-quorum-b0574bb60700 (Accessed: 23 November 2018).

Dijck, J. van (2013) *The culture of connectivity: A critical history of social media*. Oxford: Oxford University Press.

Dikeç, M. (2012) ‘Space as a mode of political thinking’, *Geoforum*, 43, pp. 669–676.

Dodge, M. and Kitchin, R. (2011) *Code / Space: Software and Everyday Life*. Cambridge, Massachusetts and London, England: MIT Press.

Dwork, C. and Naor, M. (1992) ‘Pricing via Processing or Combatting Junk Mail’, *Advances in Cryptology — CRYPTO’ 92*.

Dwork, C., Naor, M. and Sahai, A. (2004) ‘Concurrent zero-knowledge’, *Journal of the ACM*, 51(6), pp. 851–898.

Economist, T. (2015) ‘The great chain of being sure about things’, *The Economist*, October [online]. Available at: http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable (Accessed: 1 November 2015)

Edwards, Paul N. (2003) ‘Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems’, in Misa, T. J., Brey, P., and Feenberg, A. (eds) *Modernity and Technology*. Cambridge, MA: MIT Press, pp. 185–225.

Ehrsam, F. (2017) *Blockchain Governance: Programming Our Future*, Medium [online]. Available at: https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74 (Accessed: 1 October 2018).

Erb, K. P. (2015) *Virtual Heads Or Tails: EU Says Bitcoin Is Currency For Tax Purposes While US Disagrees*, *Forbes*. Available at: http://www.forbes.com/sites/kellyphillipserb/2015/10/23/virtual-heads-or-tails-eu-says-bitcoin-is-currency-for-tax-purposes-while-us-disagrees/ (Accessed: 6 November 2015).

Ethereum Classic (2017) *Out of the Ether: A Crisis of Irresponsible Governance Facing Ethereum Classic*, Medium [online]. Available at: https://medium.com/@classicether/out-of-the-ether-a-crisis-of-irresponsible-governance-facing-ethereum-classic-a77abdd7a9fa (Accessed: 20 October 2018).

Ethereum (2014) *Vitalik Buterin reveals Ethereum at Bitcoin Miami 2014*. YouTube. Available at: https://youtu.be/l9dpjN3Mwps (Accessed: 17 March 2015).

Ethereum Foundation (2017) *Introduction to cryptoeconomics - Vitalik Buterin*. YouTube/ Ethereum Foundation. Available at: https://youtu.be/pKqdjaH1dRo (Accessed: 7 March 2017).

Eyal, I. and Sirer, E. G. (2013) ‘Majority is not Enough : Bitcoin Mining is Vulnerable’ [online]. Available at: https://arxiv.org/pdf/1311.0243.pdf (Accessed: 5 March 2015).

Farrer, M. (2018) ‘Bitcoin bubble is bursting and has a long way to fall, economists warn’, *The Guardian*, 18 January [online]. Available at: https://www.theguardian.com/technology/2018/jan/18/bitcoin-speculative-bubble-bursting-long-way-to-fall-economists-warn (Accessed: 18 January 2018).

Feenberg, A. (1992) ‘Subversive rationalization: Technology, power, and democracy’, *Inquiry: An Interdisciplinary Journal of Philosophy*, 35(3–4), pp. 301–322.

Feenberg, A. (1999) *Questioning Technology*. London and New York: Routledge.

Filippi, P. De (2013) ‘Bitcoin: a regulatory nightmare to a libertarian dream’, *Internet Policy Review*, 3(2), p. 43.

Filippi, P. De (2014) ‘Primavera De Filippi on Ethereum: Freenet or Skynet?’ YouTube/ The Berkman Klein Center for Internet & Society. Available at: https://youtu.be/slhuidzccpI (Accessed: 17 March 2015).

Filippi, P. De and Wright, A. (2015) ‘Decentralized blockchain technology and the rise of Lex Cryptographia’ [online]. Available at: http://ssrn.com/abstract=2580664 (Accessed: 9 February 2016).

Finklea, K. (2017) *Dark Web* [online]. Available at: https://fas.org/sgp/crs/misc/R44101.pdf (Accessed: 4 May 2018).

Gabbatiss, J. (2018) ‘Expanding Bitcoin use will push global warming above 2C in two decades, finds study’, *The Independent*, 29 October [online]. Available at: https://www.independent.co.uk/environment/bitcoin-climate-change-global-warming-cryptocurrency-mining-electricity-a8607036.html (Accessed: 29 October 2018).

Galloway, A. (2004) *Protocol: How Control Exists After Decentralization*. Cambridge and London: The MIT Press.

Galloway, A. (2005) ‘Design in the parliament of things’, *Design Engaged*.

Garay, J., Kiayias, A. and Leonardos, N. (2015) ‘The Bitcoin backbone protocol: Analysis and applications’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9057, pp. 281–310.

Gencer, A. E. *et al.* (2018) ‘Decentralization in Bitcoin and Ethereum Networks’ [online]. Available at: https://fc18.ifca.ai/preproceedings/75.pdf (Accessed 5 February 2019).

Gerard, D. (2017) *Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts*. Amazon: Gerard.

Gerbaudo, P. (2017) *The Mask and the Flag: Populism, Citizenism, and Global Protest*. Oxford: Oxford University Press.

Gibson-Graham, J. K.(1996). *The End of Capitalism (As We Knew It): A Feminist Critique of Political Economy*. Minnesota: University of Minnesota Press.

Gibson-Graham, J. K. (2008) ‘Diverse economies: Performative practices for “other worlds”’, *Progress in Human Geography*, 32(5), pp. 613–632. doi: 10.1177/0309132508090821.

Golumbia, D. (2015) ‘Bitcoin as Politics: Distributed Right-Wing Extremism’, in Lovink, G., Tkacz, N., and Vries, P. De (eds) *An Intervention in Digital Economy*. #10. Amsterdam: Institute of Network Cultures.

Golumbia, D. (2016) *The Politics of Bitcoin, Software as Righ-Wing Extremism*. Minneapolis: University of Minnesota Press.

Greenfield, A. (2017) *Raical Technologies: The Design of Everyday Life*. London and New York: Verso.

Greenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Picador.

Grigg, I. (2005) *Triple Entry Accounting* [online]. Available at: iang.org/papers/triple_entry.html (Accessed: 9 October 2015).

Grigg, I. (2014) ‘A quick history of Cryptocurrencies BBTC - Before Bitcoin’, *Bitcoin Magazine*, April [online]. Available at: https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630 (Accessed: 7 May 2014).

Grigg, I. (2016) *Satoshi is dead - long live Satoshi - team leader comes out* personal blog [online]. Available: http://financialcryptography.com/mt/archives/001593.html (Accessed: 01-May-2016).

Gupta, V. (2015) *'Tell me who you are, Identity, institutional memory, and the persistent illusion of the self'*, Medium [online]. Available at: https://medium.com/@ConsenSys/tell-me-who-you-are-258268bf3180 (Accessed 20 January 2016).

Gutiérrez-rubí, A. (2011) *Tecnopolítica*. Available from: https://www.gutierrez-rubi.es/2014/11/21/tecnopolitica-2/ (Accessed: May 2015).

Hagelstrom, M. (2016) 'Why Bitcoin's Block Size Debate is a Proxy War', *Coindesk*, March. Available at: http://www.coindesk.com/bitcoin-block-size-proxy-war/.

Haiven, M. (2018) *Art After Money, Money After Art: Creative Strategies Against Financialization*. London: Pluto Press.

Halpin, H. and Thompson, H. S. (2009) 'Social Meaning on the Web: From Wittgenstein to Search Engines', *IEEE Intelligent Systems*, 24.

Haraway, D. (1991) 'A cyborg manifesto: Science, Technology, and the Socialist-Feminism in the Late Twentieth Century', in *Simians, Cyborgs and Women, The Reinvention of Nature*. London: Free Association Books.

Haraway, D. (1992) 'The Promises of Monsters: A Regenerative Politics For Inappropriate/d Others', in Grossberg, L., Nelson, C., and Treichler, P. A. (eds) *Cultural studies*. New York: Routledge, pp. 295–337.

Haraway, D. (2016) *Staying With the Trouble: Making kin in the Chthulucene*. Durham and London: Duke University Press.

Harvey, G. (2005) 'Animism - A Contemporary Perspective', *Encyclopedia of Religion and Nature*, pp. 81–83.

Hayles, K. (2005) *My Mother Was a Computer, digital subjects and literary texts*. Chicago and London: University of Chicago Press.

Hayles, N. K. (1999) *How We Became Posthuman*. Chicago and London: The University of Chicago Press.

Hearn, M. (2015) *Why is Bitcoin Forking?* Medium [online]. Available at: https://medium.com/faith-and-future/why-is-bitcoin-forking-d647312d22c1 (Accessed: 14 September 2015).

Hearn, M. (2016) *'The resolution of the Bitcoin experiment',* Medium [online]. Available at: https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.tfg5io448 (Accessed: 14 January 2016).

Herian, R. (2016) *Anything but disruptive: blockchain, capital and a case of fourth industrial age enclosure – Part I*, *Critical Legal Thinking*. Available at:

http://criticallegalthinking.com/2016/10/18/anything-disruptive-blockchain-capital-case-fourth-industrial-age-enclosure-part/ (Accessed: 21 October 2016).

Herley, C. (2009) 'So long, and no thanks for the externalities: the rational rejection of security advice by users', *Security*, pp. 133–144.

Higgins, S. (2017) 'As India Goes Cashless, its Central Bank Researches Blockchain', *Coindesk*, January [online]. Available at: https://www.coindesk.com/india-goes-cashless-central-bank-researches-blockchain (Accessed: 9 February 2019).

Hughes, E. (1993) *A cypherpunk manifesto* [online]. Available at: https://www.activism.net/cypherpunk/manifesto.html (Accessed: 15 October 2014).

IamSatoshi (2015) *CoinScrum: QA with Gavin Andresen and Mike Hearn*. YouTube. Available at: https://youtu.be/RIafZXRDH7w (Accessed: 5 June 2016).

Ingold, T. (2000) *The Perception of the Environment, essays on livlihood, dwelling and skill*. London and New York: Routledge.

Ingold, T. (2011) *Being Alive: Essays on Movement, Knowledge and Description*. London and New York: Routledge.

Innes, A. (1914) 'The Credit Theory of Money', *The Banking Law Journal*, 31(January), pp. 151–68.

Ito, J. (2017) 'Resisting Reduction: A Manifesto Designing our Complex Future with Machines', *Journal of Design and Science* [online]. Available at: https://jods.mitpress.mit.edu/pub/resisting-reduction (Accessed: 8 November 2018).

Jentzsch, C. (2016) 'Decentralized autonomous organization to automate governance' *Slock.it* [online]. Available at: https://download.slock.it/public/DAO/WhitePaper.pdf (Accessed: 7 August 2016).

Johnson, D. G. and Noorman M. (2014) Artefactual Agency and Artefactual Moral Agency in *The Moral Status of Technical Aftefacts*, Kroes, P. and Verbeek, P.-P. (eds) Springer

Käll, J. (2018) 'Blockchain Control', *Law and Critique*. Springer Netherlands, 29(2), pp. 133–140.

Kennedy, J. *et al.* (2001) *Swarm Intelligence*. San Diego, London, San Francisco: Academic Press.

Kiayias, A. (2015) 'Fair and Robust Multi-Party Computation using a Global Transaction Ledger' [online]. Available at: https://eprint.iacr.org/2015/574 (Accessed October 2015) .

Kitchin, R. (2014) 'Big Data, new epistemologies and paradigm shifts', *Big Data & Society*, 1(1), pp. 1–12.

Kozinets, R. V (2015) *Netnography Redefined*. 2nd edn. London, New Delhi, Singapore: SAGE.

Kreutler, K. (2018) 'The Byzantine Generalization Problem: Subtle Strategy in the Context of Blockchain Governance', *Technosphere Magazine*, August [online]. Available at:

https://technosphere-magazine.hkw.de/p/The-Byzantine-Generalization-Problem-Subtle-Strategy-in-the-Context-of-Blockchain-Governance-8UNNcM8VShTpBGWRuob1GP (Accessed: 19 August 2018).

Laclau, E. and Mouffe, C. (2001) *Hegemony and Socialist Strategy*. London and New York: Verso.

Lamport, L., Shostak, R. and Pease, M. (1982) 'The Byzantine Generals Problem', *ACM Transactions on Programming Languages and Systems*, 4(3), pp. 382–401.

Langley, P. and Leyshon, A. (2016) 'Platform capitalism: the intermediation and capitalization of digital economic circulation', *Finance and Society*, 2(1).

Latour, B. (1992) 'Where are the missing masses? The sociology of a few mundane artifacts', in Bijker, W. and Law, J. (eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, MA: MIT Press, pp. 225–258.

Latour, B. (2005) *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press.

Law, J. (2016) 'STS as method', *Handbook of Science and Technology Studies (4th edition)*, June [online]. Available at: http://www.heterogeneities.net/publications/Law2015STSAsMethod.pdf (Accessed: 8 February 2017).

Lessig, L. (1999) *Code and other laws of cyberspace*. New York: Basic Books.

Levy, K. E. C. (2017) 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law', *Engaging Science, Technology, and Society*, 3.

Lo, S. and Wang, J. C. (2014) *Bitcoin as Money?* [online]. Available at: https://www.bostonfed.org/-/media/Documents/Workingpapers/PDF/cpp1404.pdf (Accessed: 10 March 206)

Malone, D. and O'Dwyer, K. J. (2014) 'Bitcoin Mining and its Energy Footprint', *China-Ireland International Conference on Information and Communications Technologies* (ISSC 2014/CIICT 2014).

Manski, S. and Manski, B. (2018) 'No Gods , No Masters , No Coders ? The Future of Sovereignty in a Blockchain World', *Law and Critique*. Springer Netherlands, 29(2), pp. 151–162.

Martin, J. (2014) 'Lost on the Silk Road : Online drug distribution and the " cryptomarket "'. *Criminology & Criminal Justice*, 14(3), pp. 351-367.

Matonis, J. (2012) 'WikiLeaks Bypasses Financial Blockade With Bitcoin', *Forbes*, August. Available at: https://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin/#7b433daf7202 (Accessed: 17 August 2016).

McGee, M. C. (1980) 'The ideograph: A link between rhetoric and ideology', *Quarterly Journal of Speech*, 66.

McKinsey (2016) *How blockchains could change the world* [online]. Available at: https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world.

McKittrick, K. (2014) ‘Mathematics Black Life’, *The Black Scholar*, 44(2), pp. 16–28.

McMillan, R. (2014) ‘The Inside Story of Mt. Gox, Bitcoin’s $460 Million Disaster’, *Wired*, March [online]. Available at: https://www.wired.com/2014/03/bitcoin-exchange/ (Accessed: 9 October 2015).

Meiklejohn, S. *et al*. (2013) ‘A fistful of Bitcoins: Characterizing payments among men with no names’, *Proceedings of the Internet Measurement Conference - IMC ’13*, pp. 127–140.

Meiklejohn, S. (2018) ‘Top ten obstacles along distributed ledgers path to adoption’, *IEEE Security and Privacy*. IEEE, 16(4), pp. 13–19.

Merkle, R. C. (1979) *Secrecy, Authentication and Public Key Systems*. Available at: https://www.merkle.com/papers/Thesis1979.pdf (Accessed 14 June 2015).

Merkle, R. C. (1982) ‘Method of Providing Digital Signatures’, *US Patent* [online]. Available at: https://www.google.com/patents/US4309569 (Accessed: 2 June 2016).

Mittal, S. (2012) *Is Bitcoin Money? Bitcoin and Alternate Theories of Money* [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2434194 (Accessed: 7 June 2016).

Morgan, D. (2017) *The Great Bitcoin Scaling Debate - A Timeline*, Hackernoon [online]. Available at: https://hackernoon.com/the-great-bitcoin-scaling-debate-a-timeline-6108081dbada (Accessed: 26 September 2018).

Mouffe, C. (1993) *The Return of the Political*. London and New York: Verso.

Mouffe, C. (2005) *On The Political*. London and New York: Routledge.

Mouffe, C. (2012) ‘Space, Hegemony and Radical Critique’, *Spatial Politics: Essays for Doreen Massey*, pp. 19–31. doi: 10.1002/9781118278857.ch1.

Musiani, F. *et al.* (2016) *Internet Science Vocabulary and Key Questions* [online]. Available at: https://nextleap.eu/deliverables/D2.1-interdisciplinary.pdf (Accessed: 20 October 2016).

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf (Accessed: 4 October 2011).

Nakamoto, S., Bridle, J. and Brekke, J. K. (2019) *The White Paper*. Edited by B. Vickers. London: Ignota.

Narayanan, A. and Möser, M. (2017) ‘Obfuscation in Bitcoin: Techniques and Politics’ [online]. Available at: http://arxiv.org/abs/1706.05432 (Accessed: 7 January 2018).

Naughton, J. (2016) ‘Is Blockchain the most important IT invention of our age?’, *The Guardian*, 24 January [online]. Available at: http://www.theguardian.com/commentisfree/2016/jan/24/blockchain-bitcoin-technology-most-important-tech-invention-of-our-age-sir-mark-walport (Accessed: 25 January 2016).

Noorman, M. (2014) ‘Responsibility Practices and Unmanned Military Technologies’, *Science and Engineering Ethics*, 20(3), pp. 809–826.

O’Brien, M. (2015) ‘Bitcoin isn’t the future of money — it’s either a Ponzi scheme or a pyramid scheme’, *The Washington Post*, 8 June.

O'Dwyer, R. (2015) ‘The Revolution will (not) be decentralised : Blockchains’ [online]. Available at: https://blog.p2pfoundation.net/the-revolution-will-not-be-decentralised/2015/03/23.

Oram, A. (ed.) (2001) *Peer-to-Peer, Harnessing the Benefits of Disruptive Technology*. Beijing, Cambridge, Farham, Koln, Paris, Sebastopol, Taipei and Tokyo: O’Reilly.

Pagliery, J. (2015) ‘Bitcoin fallacy led to Silk Road founder’s conviction’, *CNN Business*, 5 February [online]. Available at: https://money.cnn.com/2015/02/05/technology/security/bitcoin-silk-road/index.html (Accessed: 10 May 2016).

Papadopoulos, D. (2011) ‘Alter-ontologies: Towards a constituent politics in technoscience’, *Social Studies of Science*, 41(2), pp. 177–201.

Pasquale, F. (2010) ‘Restoring Transparency To Automated Authority’, *Journal on Telecomm and high tech*, 9, pp. 235–254.

Pasquale, F. (2017) ‘Two Narratives of Platform Capitalism’, *Yale Law & Policy Review*, 35(1).

Pazaitis, A., Kostakis, V. and Bauwens, M. (2017) ‘Digital economy and the rise of open cooperativism: the case of the Enspiral Network’, *Transfer*, 23(2), pp. 177–192.

Peters, G., Panayi, E. and Chapelle, A. (2015) ‘Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective’, *Ssrn*, 3(3).

Poon, J. and Dryja, T. (2015) ‘The Bitcoin Lightning Network’ [online]. Available at: https://lightning.network/lightning-network-paper.pdf (Accessed 4 April 2016).

Posner, E. A. (2013) ‘Fool’s Gold Bitcoin is a Ponzi scheme—the Internet’s favorite currency will collapse’, Slate 11 April [online]. Available at: https://slate.com/news-and-politics/2013/04/bitcoin-is-a-ponzi-scheme-the-internet-currency-will-collapse.html (Accessed 5 June 2015).

Preneel, B. (2010) ‘The first 30 years of cryptographic hash functions and the NIST SHA-3 competition’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5985 LNCS, pp. 1–14.

Prieto, P. and Duran, E. (2015) *FairCoop: virus of cooperation infects a new economy*, *ROAR* [online]. Available at: http://roarmag.org/2015/01/faircoop-cooperation-new-economy/ (Accessed: 13 September 2015).

Rancière, J. (2006) *The Politics of Aesthetics*. London and New York: Continuum.

Rancière, J. (2010) *Dissensus, on Politics and Aesthetics*. Edited by S. Corcoran. London and New York: Continuum.

Reijers, W. and Coeckelbergh, M. (2016) 'The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies', *Philosophy & Technology*. Philosophy & Technology, 7.

Reijers, W., O'Brolcháin, F. and Haynes, P. (2016) 'Governance in Blockchain Technologies & Social Contract Theories', *Ledger*, 1(0), pp. 134–151.

Richards, C. (2015) 'Greece at a financial cross-roads and a practical solution could be Bitcoin', *Cointelegraph*, January [online]. Available at: https://cointelegraph.com/news/greece-at-a-financial-cross-roads-and-a-practical-solution-could-be-bitcoin (Accessed: 5 January 2016).

Rifkin, J. (2014) *The zero marginal cost society*. Palgrave Macmillan.

Rivlin, B. (2016) *Charles Hoskinson Tells Us Why He Is 100% ETC*, *Eth News* [online]. Available at: https://www.ethnews.com/charles-hoskinson-tells-us-why-he-is-100-etc (Accessed: 22 November 2018).

Rizzo, P. (2014) *Bitcoin and Litecoin Top Sources of WikiLeaks Donations*, *Coindesk* [online]. Available at: http://www.coindesk.com/bitcoin-litecoin-source-wikileaks-donations/ (Accessed: 3 September 2015).

Robinson, E. and Leising, M. (2015) 'Blythe Masters Tells Banks Why Blockchain Changes Everything', *Bloomberg*, September [online]. Available at: https://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything (Accessed: 8 October 2015).

Robleh, A. *et al.* (2014) 'Innovations in payment technologies and the emergence of digital currencies.', *Bank of England Quarterly Bulletin*, Q3(3), pp. 262–276.

Rogaway, P. (2015) 'The Moral Character of Cryptographic Work' [online]. Available at: https://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf (Accessed: 28 March 2016).

Rogers, G. *et al.* (2015) *D5 . 3 Implementation of collaborative policy-making tool*. Available at: http://dcentproject.eu/wp-content/uploads/2015/07/D5.3.pdf (Accessed: 19 January 2016).

Roio, D. *et al.* (2015) *D4 . 4 Design of Social Digital Currency*. Available at: https://dcentproject.eu/wp-content/uploads/2015/03/design_of_social_digital_currency_publication.pdf (Accessed: 25 January 2016).

Roio, D. (2018) *Algorithmic Sovereignty*. University of Plymouth.

Roio, D. J. (2013) *Bitcoin, the end of the Taboo on Money*. Planetary Collegium.

Roio, D. and Sachy, M. (2015) 'D-CENT: Implementation of digital social currency infrastructure', (610349). Available at: https://dcentproject.eu/wp-content/uploads/2015/09/D5.5-Implementation-of-digital-social-currency-infrastructure-.pdf (Accessed: 24 January 2016).

Saberhagen, N. Van (2013) 'CryptoNote v 2.0' [online]. Available at: https://cryptonote.org/whitepaper.pdf (Accessed: 19 December 2018).

Scholz, T. (2016) ‘Platform Cooperativism. Challenging the Corporate Sharing Economy’. Rosa Luxemburg Stiftung. Available at: http://ictlogy.net/bibliography/reports/projects.php?idp=3111 (Accessed: 23 November 2018).

Schwartz, J. (2013) ‘Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide’, *The New York Times*, January [online]. Available at: https://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html (Accessed: 17 July 2016).

Scott, B. (2014) ‘Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain’, *e-international relations* [online]. Available at: https://www.e-ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/ (Accessed: 11 June 2015).

Scott, B. (2016) ‘Working Paper 2016-1 How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance ?’, UNRISD [online]. Available at: http://www.unrisd.org/80256B3C005BCCF9/httpNetITFramePDF?ReadForm&parentunid=196AEF663B617144C1257F550057887C&parentdoctype=paper&netitpath=80256B3C005BCCF9/(httpAuxPages)/196AEF663B617144C1257F550057887C/$file/Brett Scott.pdf (Accessed: 18 March 2017).

Scott, B. (2018) *These 5 Rebel Movements Want To Change How Money Works*, *Peer-to-peer Foundation* [online]. Available at: https://blog.p2pfoundation.net/these-5-rebel-movements-want-to-change-how-money-works/2018/09/20 (Accessed: 20 November 2018).

Seaver, N. (2014) ‘Knowing algorithms’, *Media in Transition*, 8(April 2013), pp. 1–12.

Sirer, E. G. (2016) *Thoughts on The DAO Hack*, *Hacking, Distributed*. Available at: http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/.

Slock.it (2016) ‘For a Universal Sharing Network, the Ethereum Computer Reference Design and its Ecosystem of Applications’ (no longer available. Contact thesis author for archived pdf).

Smith, C. E. (2010) ‘Net Neutrality, Full Throttle: Regulation of Broadband Internet Service Following the Comcast/Bittorrent Dispute’, *Santa Clara Law Review*, 50(2), p. 569.

Smolenski, N. (2016) *Identity and Digital Self-Sovereignty A New Paradigm for Sovereignty on the High Seas*, Medium [online]. Available at: https://medium.com/learning-machine-blog/identity-and-digital-self-sovereignty-1f3faab7d9e3 (Accessed: 31 January 2018).

Söderberg, J. and Daoud, A. (2012) ‘Atoms want to be free too! expanding the critique of in-tellectual property to physical goods’, *TripleC*, 10(1), pp. 66–76.

Srinivasan, B. S. (2017) ‘Quantifying Decentralization’ [online]. Available at: https://news.earn.com/quantifying-decentralization-e39db233c28e (Accessed: 3 April 2018).

Srnicek, N. (2017) *Platform Capitalism*. Cambridge and Malden: Polity Press.

Star, S. L. (1999) ‘The Ethnography of Infrastructure’, *American Behavioral Scientist*, 43(3), pp. 377–391.

Steiner, J. (2018) ‘What the heck is web 3.0 anyway’, *Forbes*, October [online]. Available at: https://www.forbes.com/sites/juttasteiner/2018/10/26/what-the-heck-is-web-3-0-anyway/ (Accessed 26 October 2018).

Stolfi, J. (2016) ‘Letter from Jorge Stolfi to the US Securities and Exchange Commission’. US Securities and Exchange Commission.

Strathern, M. (1996) ‘Cutting the Network’, *The Journal of the Royal Anthropological Institute*, 2(3), pp. 517–535.

Svensson, P. (2007) ‘Comcast blocks some Internet traffic’, *MSNBC*, 19 October [online]. Available at: https://web.archive.org/web/20110507232209/http://www.msnbc.msn.com/id/21376597/ (Accessed; 17 December 2018).

Swan, M. (2015) *Blockchain, blueprint for a new economy*. Beijing, Cambridge, Farham, Koln, Sebastopol and Tokyo: O’Reilly.

Szabo, N. (1997) *The Idea of Smart Contracts*, Personal blog [online]. Available at: https://perma.cc/V6AZ-7V8W (Accessed: 17 December 2017).

Szabo, N. (2014) *The dawn of trustworthy computing* [online]. Available at: http://unenumerated.blogspot.dk/2014/12/the-dawn-of-trustworthy-computing.html (Accessed: 8 July 2015).

Tapscott, D. and Tapscott, A. (2018) *Blockchain Revolution, how the technology behind Bitcoin and other cryptocurrencies is changing the world*. New York: Portfolio/Penguin.

Terranova, T. (2004) *Network Culture. Politics for the Information Age*. London: Pluto Press.

Troncoso, C., Isaakidis, M., Danezis, G. and Halpin, H. (2017) ‘Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments’, *Proceedings on Privacy Enhancing Technologies*, (4), pp. 307–329.

Tual, S. (2016a) ‘A Primer to Decentralized Autonomous Organizations (DAOs)’, Medium [online]. Available at: https://blog.slock.it/a-primer-to-the-decentralized-autonomous-organization-dao-69fb125bd3cd#.19guhyb3v (Accessed: 29 July 2016).

Tual, S. (2016b) ‘DAOs, or how to Replace Obsolete Governance Models’, Medium [online]. Available at: https://blog.slock.it/daos-or-how-to-replace-both-the-kickstarter-and-token-presale-models-1b2b8898d6e7#.vgno69gva (Accessed: 29 July 2016).

Tual, S. (2016c) ‘The DAO Creation is now Live’, Medium [online]. Available at: https://blog.slock.it/the-dao-creation-is-now-live-2270fd23affc#.645egdvyg (Accessed: 29 July 2016).

Tual, S. (2016d) *The Ethereum Chain Hard Fork and Immutability Debate*, Medium [online]. Available at: https://blog.stephantual.com/the-ethereum-chain-hard-fork-a419b83ba753 (Accessed: 2 October 2018).

TwoBitIdiot (2017) *Bitcoin's Constitutional Crisis & Why I Support the UASF*, Medium [online]. Available at: https://medium.com/tbis-weekly-bits/bitcoins-constitutional-crisis-why-i-support-the-uasf-5b0ab325d8b6 (Accessed: 3 May 2018).

Ullman, E. (2013) *Close to the Machine: Technophilia and Its Discontents*. Pushkin Press.

Valenzuela, J. (2016) 'Arcade City: Ethereum's Big Test Drive to Kill Uber', *Cointelegraph*, March [online]. Available at: https://cointelegraph.com/news/arcade-city-ethereums-big-test-drive-to-kill-uber (Accessed: 27 October 2017).

Varoufakis, Y. (2014) *BITCOIN: A flawed currency blueprint with a potentially useful application for the Eurozone*, Personal blog [online]. Available at: https://www.yanisvaroufakis.eu/2014/02/15/bitcoin-a-flawed-currency-blueprint-with-a-potentially-useful-application-for-the-eurozone/ (Accessed: 11 December 2018).

Vavilov, V. (2016) 'Keep Calm and Bitcoin On', Medium [online]. Available at: https://medium.com/@BitFuryGroup/keep-calm-and-bitcoin-on-4f29d581276#.ir8smlpp1 (Accessed: 28 January 2016).

Vidan, G. and Lehdonvirta, V. (2018) 'Mine the gap: Bitcoin and the maintenance of trustlessness', *New Media and Society*, (May 2015), pp. 1–18.

Vigna, P. and Casey, M. J. (2015) 'Cryptocurrency, How Bitcoin and Digital Money are Challenging the Global Economic Order'. London: The Bodley Head.

Vigna, P. and Casey, M. J. (2018) *The Truth Machine, the blockchain and the future of everything*. London: HarperCollins.

Voge, C. (2018) 'Where could Bitcoin succeed as currency? In a failed state', *Wired*, March [online]. Available at: https://www.wired.com/story/where-could-bitcoin-succeed-as-a-currency-in-a-failed-state/ (Accessed: 6 January 2019).

Vorick, D. (2018) *The State of Cryptocurrency Mining* [online]. Available at: https://blog.sia.tech/the-state-of-cryptocurrency-mining-538004a37f9b (Accessed: 2 October 2018).

Walport, M. (2016) *Distributed Ledger Technology: beyond block chain*. London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (Accessed: 8 June 2017).

Wirdum, A. van (2015a) 'Segregated Witness, Part 1: How a Clever Hack Could Significantly Increase Bitcoin's Potential', *Bitcoin Magazine*, December [online]. Available at: https://bitcoinmagazine.com/articles/segregated-witness-part-how-a-clever-hack-could-significantly-increase-bitcoin-s-potential-1450553618 (Accessed: 4 January 2016).

Wirdum, A. Van (2015b) 'Segregated Witness, Part 2: Why You Should Care About a Nitty-Gritty Technical Trick', *Bitcoin Magazine*, December [online]. Available at:

https://bitcoinmagazine.com/articles/segregated-witness-part-why-you-should-care-about-a-nitty-gritty-technical-trick-1450827675 (Accessed: 4 January 2016).

Wirdum, A. van (2015c) 'Segregated Witness, Part 3: How a Soft Fork Might Establish a Block-Size Truce (or Not)', *Bitcoin Magazine*, December [online]. Available at: https://bitcoinmagazine.com/articles/segregated-witness-part-how-a-soft-fork-might-establish-a-block-size-truce-or-not-1451423607 (Accessed: 4 January 2016).

Wirdum, A. van (2016a) 'A Primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol', *Bitcoin Magazine*, September [online]. Available at: https://bitcoinmagazine.com/articles/a-primer-on-bitcoin-governance-or-why-developers-aren-t-in-charge-of-the-protocol-1473270427/ (Accessed: 8 October 2016).

Wirdum, A. van (2016b) 'On Consensus, or Why Bitcoin's Block-Size Presents a Political Trade-Off', *Bitcoin Magazine*, January [online]. Available at: https://bitcoinmagazine.com/articles/on-consensus-or-why-bitcoin-s-block-size-presents-a-political-trade-off-1452887468 (Accessed: 4 February 2016).

Wirdum, A. van (2016c) *Why Some Changes to Bitcoin Require Consensus: Bitcoin's 4 Layers*, *Bitcoin Magazine* [online]. Available at: https://bitcoinmagazine.com/articles/why-some-changes-to-bitcoin-require-consensus-bitcoin-s-layers-1456512578/ (Accessed: 4 June 2016).

Wirdum, A. van (2017) *A Bitcoin Beginner's Guide to Surviving the BIP 148 UASF*, *Bitcoin Magazine*, May [online]. Available at: https://bitcoinmagazine.com/articles/bitcoin-beginners-guide-surviving-bip-148-uasf/ (Accessed: 3 June 2017).

Wood, G. (2014c) 'Ethereum: a secure decentralised generalised transaction ledger EIP-150 Revision'. Ethereum. Available at: https://gavwood.com/paper.pdf (Accessed: 8 July 2015).

Wood, G. (2014b) *ĐApps: What Web 3.0 Looks Like*, *Insights Into A Modern World,* Personal blog [online]. Available at: http://gavwood.com/dappsweb3.html (Accessed: 3 June 2017).

Wuille, P. (2015) 'Segregated Witness' Bitcoin Core [online. Available at: https://bitcoincore.org/en/2016/01/26/segwit-benefits/ (Accessed: 4 March 2016).

Yusoff, K. (2013a) 'Insensible worlds: Postrelational ethics, indeterminacy and the (k)nots of relating', *Environment and Planning D: Society and Space*, 31(2), pp. 208–226.

Yusoff, K. (2013b) 'Geologic life: Prehistory, climate, futures in the Anthropocene', *Environment and Planning D: Society and Space*, 31(5), pp. 779–795.

Yusoff, K. (2017) 'Epochal Aesthetics: Affectual Infrastructures of the Anthropocene', *e-flux*, March [online]. Available at: https://www.e-flux.com/architecture/accumulation/121847/epochal-aesthetics-affectual-infrastructures-of-the-anthropocene/ (Accessed: 9 January 2019).

Zamfir, V. (2016) *Dear Ethereum Community*, Medium [online]. Available at: https://medium.com/@Vlad_Zamfir/dear-ethereum-community-acfa99a037c4 (Accessed: 7 September 2017).

Zamfir, V. (2017) *Against on-chain governance, Refuting (and rebuking) Fred Ehrsam's governance blog*, Medium [online]. Available at: https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca (Accessed: 1 October 2018).

Zamfir, V. (2018) *Blockchain governance 101*, Medium [online]. Available at: https://medium.com/@Vlad_Zamfir/blockchain-governance-101-eea5201d7992 (Accessed: 2 October 2018).

Zuboff, S. (2015) 'Big other: surveillance capitalism and the prospects of an information civilization', *Journal of Information Technology*, 30(1).

Zurko, M. E. and Simon, R. T. (1996) 'User-centered security', *Proceedings of the 1996 workshop on New security paradigms - NSPW '96*, pp. 27–33.

Appendix: Empirical sources

Table 1: interviews

Interviews	Date	Topic
Denis Jaromil Roio, Dyne	28.01.2016	The politics of the Bitcoin community and clarifying factions in the early days of the block size conflict.
Vlad Zamfir, Ethereum	20.07.2016	Ethereum DAO hack, forking and governance in decentralized systems.
Enric Duran, Faircoin	29.11.2015	Faircoin idea, history and project.
Matthew Slater, currency activist	04.03.2016	Faircoin community decision-making processes, “internal” community versus “external” market-based exchange rates.
Pikette, Aurea Social Faircoin welcome committee	07.03.2016	The Aurea Social FairCoop centre, affiliated Faircoop projects and history.
Sebas, Faircoin Girona local node	11.03.2016	Girona Faircoin node, Faircoin governance structure and relationships to FaircCoop and other “Fair” projects.
Ale, Faircoin Barcelona local node	01.11.2016	Faircoin local nodes and organizational issues.

I conducted only a limited number of interviews early on in my fieldwork. This was because it quickly became clear that there was substantial work to do in gathering and analysing already available online interviews and material before I would be able to develop meaningful questions beyond the existing information. And so my empirical focus for this PhD has been online community discussions, email lists, code repositories, statements and blogs of key figures. The majority of the empirical work consisted in studying the development and online discussions around the technical architectures of what was still a very new and emerging set of projects and communities. These are detailed below.

Table 2: online sources and empirical material

Source	Reasoning	Material
GitHub A platform for managing and collaborating on code projects	An important indicator of how alive a project might be was their respective GitHub repositories: how recently these had been modified, how many contributors and discussions there were.	Bitcoin https://github.com/bitcoin/bitcoin Bitcoin cash https://github.com/bitcoincashorg/bitcoincash.org Ethereum https://github.com/ethereum Ethereum Classic https://github.com/ethereumclassic and https://github.com/ethereumproject Faircoin https://github.com/faircoin/faircoin
Email lists	Changes to the Bitcoin protocol would be discussed on the Bitcoin developers' mailing list. The discussion list is for broader Bitcoin related discussions and the SegWit list is for	Bitcoin developers mailing list https://lists.linuxfoundation.org/pipermail/bitcoin-dev/ Bitcoin email list for discussions https://lists.linuxfoundation.org/pipermail/bitcoin-discuss/ Bitcoin email list for segwit2x https://lists.linuxfoundation.org/mailman/listinfo/bitcoin-segwit2x
Medium publishing platform	The blog platform Medium became a main site where projects and key individuals in the industry would articulate their reasons for pursuing various development pathways and explain the ideas behind their work.	In particular but not limited to: Vitalik Buterin, founder of Ethereum https://medium.com/@VitalikButerin Vlad Zamfir, Ethereum developer, developer of DAO fork and proof-of-stake https://medium.com/@Vlad_Zamfir Stephan Tual, founder of Ethereum company Slock.it https://medium.com/@stephantual Valery Vavilov, CEO of Bitfury https://medium.com/@valeryvavilov Mike Hearn, ex-Bitcoin developer, https://medium.com/@OctSkyward Hackernoon https://medium.com/@hackernoon
Twitter	Twitter is another key site where many discussions, organizing and commentary in the cryptocurrency and blockchain community. It was	In particular but not limited to: Peter Todd, Bitcoin developer, https://twitter.com/peterktodd; Gavin Andresen, Bitcoin developer https://twitter.com/gavinandresen; Jonas Schnelli, Bitcoin developer,

	a good place to get a sense of the main disputes and debates, and how much engagement there was with different projects. Where I have used quotes or explicitly drawn on statements on twitter these are referenced in the text. Discussions also provided a more general background context to my understanding of the blockchain community. Listing these key profiles here is intended to make visible the source of my understanding of the dynamics and discussions in the blockchain community such that my assessments and descriptions might be scrutinized and so that, in the eventuality of any important omissions, these might be can be highlighted.	https://twitter.com/_jonasschnelli_; Matt Corallo, Bitcoin developer, https://twitter.com/TheBlueMatt; Jeff Garzik, Bitcoin developer https://twitter.com/jgarzik; Jon Matonis, Bitcoin Foundation, https://twitter.com/jonmatonis; Adam Back, from Bitcoin company Blockstream https://twitter.com/adam3us; Bitcoin company Blockstream, https://twitter.com/Blockstream; Bitcoin Core project, https://twitter.com/bitcoincoreorg; Amir Taaki, Bitcoin and darkwallet https://twitter.com/Narodism; Denis Jaromil Roio, Bitcoin and Dyne, https://twitter.com/jaromil; Andreas Antonopoulos, Bitcoin advocate, https://twitter.com/aantonop; BitNovosti, Bitcoin news for Russian speaking Bitcoin communities, https://twitter.com/bit_novosti; Contentious, self-proclaimed inventor of Bitcoin, Craig Wright, https://twitter.com/ProfFaustus; Jameson Lopp, Bitcoin node counter and prolific commentator https://twitter.com/lopp; Chandler Guo, Bitcoin miner and investor https://twitter.com/ChandlerGuo; Jihan Wu, Bitmain, Bitcoin mining hardware company https://twitter.com/JihanWu ; Roger Ver, Bitcoin advocate, https://twitter.com/rogerkver; Izabella Kaminska, Financial Times journalist and prominent critic of cryptocurrencies https://twitter.com/izakaminska; Stacy Herbert, broadcaster of the Keiser Report, early adopter and supporter of cryptocurrencies, https://twitter.com/stacyherbert; Max Keiser of the Keiser Report, early adopter and supporter of cryptocurrencies, https://twitter.com/maxkeiser; Aaron van Wirdum, cryptocurrency journalist, https://twitter.com/AaronvanW; Tuur Demeester, Bitcoin advocate, https://twitter.com/TuurDemeester; Jimmy Song, Bitcoin advocate and developer https://twitter.com/jimmysong; Elizabeth Stark, Bitcoin entrepreneur, https://twitter.com/starkness; Vitalik Buterin, founder of Ethereum, https://twitter.com/VitalikButerin; Joseph Lubin, co-founder Ethereum, founder of ConsenSys https://twitter.com/ethereumJoseph; Ethereum company ConsenSys, https://twitter.com/ConsenSys; Jutta Steiner, co-founder Ethereum, CEO of Parity Tech, https://twitter.com/jutta_steiner; Ethereum web 3.0 company Parity Tech, https://twitter.com/ParityTech; Vlad Zamfir, Ethereum developer https://twitter.com/VladZamfir; Gavin Wood, co-founder Ethereum,

		https://twitter.com/gavofyork; Karl Floersch, Ethereum developer, https://twitter.com/karl_dot_tech; Nick Szabo, smart contracts inventor https://twitter.com/NickSzabo4; Jessi Baker, founder of Provenance, a company using Ethereum, https://twitter.com/jessibaker; Vinay Gupta, blockchain commentator, theorist and founder of Mattereum, https://twitter.com/leashless; Primavera De Filippi, blockchain artist and founder of COALA (Coalition of Automated Legal Applications, https://twitter.com/yaoeo; Gnosis, Ethereum prediction market company, https://twitter.com/gnosisPM; Kei Kreutler, blockchain organizer, artist and educator, https://twitter.com/keikreutler; Amy Castor, blockchain journalist, https://twitter.com/ahcastor; Rhian Lewis, blockchain developer and commentator https://twitter.com/rhian_is ; Ian Grigg, blockchain entrepreneur and https://twitter.com/iang_fc; Daniel Hassan, developer of Robin Hood and Dark Crystal, https://twitter.com/dan_mi_sun; Brett Scott, author on finance and blockchain critic https://twitter.com/Suitpossum; Enric Duran, Faircoin founder, https://twitter.com/EnricDuranG; FairCoop, https://twitter.com/Fair_Coop; Thomas Konig, Faircoin developer, https://twitter.com/thokon00; Elias Haase, founder of B9Lab, https://twitter.com/8bitpal; Jackson Palmer, blockchain educator, https://twitter.com/ummjackson; Hyperledger blockchain project, https://twitter.com/Hyperledger ; Holochain non-blockchain consensus network, https://twitter.com/holochain ; Holo, non-blockchain cryptocurrency, https://twitter.com/H_O_L_O_.
Discussion forums	For Bitcoin in particular, discussion about development decisions, contentious individuals, explanations for people's actions, community responses, possible infiltration and other rumors would take place on discussion forums.	Bitcointalk, one of the very early Bitcoin discussion forums https://bitcointalk.org/index.php? Reddit: https://www.reddit.com/r/Bitcoin/ and https://www.reddit.com/r/btc/ ycombinator https://news.ycombinator.com/news
Blockchain industry	Blockchain industry websites emerged and would explain	Coindesk https://www.coindesk.com/

news outlets	new technical changes, reasoning behind as well as investment and so on.	Bitcoin magazine https://bitcoinmagazine.com/ In particular journalists Aaron van Wirdum, Amy Castor and Rachel Rose O'Leary.
Telegram group chat application	Most relevant discussions for Faircoin took place on the chat application Telegram, organized in "assemblies" for different aspects of the project.	The Faircoin assemblies were all open to join. I did not participate much beyond introducing myself, instead simply observing conversation and comparing understandings and decisions with that of other blockchain communities. The assemblies that I followed were: "FairCoop"; "FC Circular economy"; "Faircoin economy strategy"; "Bank of the commons"; "multicurrency eco-system"; "FairCoin CVN operators".
Video archive	Filmmaker Tomer Kantor made an early film about cryptocurrencies titled Ulterior States: http://www.iamsatoshi.com/. As part of making the film he conducted substantial interviews with key Bitcoin and cryptocurrency figures from very early in the development of the field, which he gave me access to.	The interviews I drew on were in particular with: Peter Todd Elizabeth Stark Andreas Antonopoulos Matt Corallo Ian Grigg

To ground the research further and get a better understanding of the people, industries and investors involved I attended local meet-ups and gatherings, initially in London.

Table 3: events

What event or place	**Why**
Coinscrum cryptocurrency and blockchain meet-ups https://www.meetup.com/coinscrum/	The London Coinscrum meet-ups are a blockchain and cryptocurrency community meet-up in London, where new projects often present their ideas and progress.

MIT Medialab and Berkman Centre for Internet and Society[1] *Blockchain Workshop* at the Millenium Hotel in Mayfair, June 2015 (documentation here: https://www.youtube.com/channel/UC9Lmf5FfNkSmYMoxhQh5ktA/videos)	The third in a series of high profile workshops, previously hosted at Stanford and Berkman/MIT, the event covered potential implications for law, governance, architecture as well as finance.
Ethereum DevCon 1, Gibson Hall, City of London November 2015 https://blog.ethereum.org/2015/09/24/devcon-is-back/	The first Ethereum developer's conference. The DevCons take place every year in different cities across the world. An early introduction to the ideas, culture and communities taking part or interested in Ethereum.
NESTA organized 2015 Future Fest	Keynote speech by the founder of Ethereum Vitalik Buterin and respondent Primavera Di Filippi and an early introduction to the ideas and culture of Ethereum.
Robin Hood London Office	The Cooperative Hedge Fund, Robin Hood, ran early experiments with blockchain technology in its architecture and governance structure and held a series of "offices", small seminars. These would gather blockchain people as well as those involved with alternative currency initiatives, academia and activism giving a sense of the more activist tendencies in the blockchain assemblage.

[1] Also sponsored by Deutsche Bank, CERSA, CNRS, LSE, UCL, Oxford University and Cambridge University, SENG School of Engineering and the Hong Kong University of Science and Technology.